TP-LINK®

User Guide

TL-WR541G

54M Wireless Router



Rev: 1.0.3

1910010061

COPYRIGHT & TRADEMARKS

Specifications are subject to change without notice. TP-LINK® is a registered trademark of TP-LINK TECHNOLOGIES CO., LTD. Other brands and product names are trademarks or registered trademarks of their respective holders.

No part of the specifications may be reproduced in any form or by any means or used to make any derivative such as translation, transformation, or adaptation without permission from TP-LINK TECHNOLOGIES CO., LTD. Copyright © 2008 TP-LINK TECHNOLOGIES CO., LTD. All rights reserved.

FCC STATEMENT



This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/ TV technician for help.

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions:

1) This device may not cause harmful interference.
2) This device must accept any interference received, including interference that may cause undesired operation.

FCC RF Radiation Exposure Statement

This equipment complies with FCC RF radiation exposure limits set forth for an uncontrolled environment. This device and its antenna must not be co-located or operating in conjunction with any other antenna or transmitter.

“To comply with FCC RF exposure compliance requirements, this grant is applicable to only

Mobile Configurations. The antennas used for this transmitter must be installed to provide a separation distance of at least 20 cm from all persons and must not be co-located or operating in conjunction with any other antenna or transmitter.”

CE Mark Warning

CE 1588 ①

This is a class B product. In a domestic environment, this product may cause radio interference, in which case the user may be required to take adequate measures.

National Restrictions

2400.0-2483.5 MHz

Country	Restriction	Reason/remark
Bulgaria		General authorization required for outdoor use and public service
France	Outdoor use limited to 10 mW e.i.r.p. within the band 2454-2483.5 MHz	Military Radiolocation use. Refarming of the 2.4 GHz band has been ongoing in recent years to allow current relaxed regulation. Full implementation planned 2012
Italy		If used outside of own premises, general authorization is required
Luxembourg	None	General authorization required for network and service supply(not for spectrum)
Norway	Implemented	This subsection does not apply for the geographical area within a radius of 20 km from the centre of Ny-Ålesund
Russian Federation		Only for indoor applications

Note: It’s not used outdoors in France.

TP-LINK®

DECLARATION OF CONFORMITY

For the following equipment:

Product Description: **54M Wireless Router, 54M Wireless AP Client Router**

Model No.: **TL-WR541G/TL-WR542G,TL-WR543G**

Trademark: **TP-LINK**

We declare under our own responsibility that the above products satisfy all the technical regulations applicable to the product within the scope of Council Directives:

Directives 1999/5/EC

The above product is in conformity with the following standards or other normative documents

ETSI EN 300 328 V1.6.1: 2004
ETSI EN 301 489-17 V1.2.1: 2002
EN 61000-3-2:2000
EN 61000-3-3:1995+A1:2001
EN60950-1:2001
EN50371:2002

Person is responsible for marking this declaration:

For and on behalf of
TP-LINK TECHNOLOGIES CO.,LTD.

Zhao Jian Jun

Authorized Signature(s)

Director of International Business

Date of Issue: **24-3-2007**

TP-LINK TECHNOLOGIES CO., LTD.
ADD: Building 7, Second Part, Honghualing Industrial Zone,
Xili town, Nanshan District, Shenzhen, China
Website: www.tp-link.com

CE

Package contents

The following contents should be found in your box:

- One TL-WR541G 54Mbps Wireless Router
- One AC power Adapter for TL-WR541G 54Mbps Wireless Router
- One Quick Installation Guide
- One Resource CD for TL-WR541G 54Mbps Wireless Router, including:
  - This Guide
  - Other Helpful Information

☞ **Note:**

Make sure that the package contains the above items. If any of the listed items are damaged or missing, please contact with your distributor.

Conventions

The router or TL-WR541G mentioned in this guide stands for TL-WR541G 54Mbps Wireless Router without any explanation.

CONTENTS

Chapter 1. Introduction 1

1.1 Overview of the Router 1

1.2 Features 1

1.3 Panel Layout 2

1.3.1 The Front Panel 2

1.3.2 The Rear Panel 4

Chapter 2. Connecting the Router 5

2.1 System Requirements 5

2.2 Installation Environment Requirements 5

2.3 Connecting the Router 5

Chapter 3. Quick Installation Guide 7

3.1 TCP/IP configuration 7

3.2 Quick Installation Guide 9

Chapter 4. Configuring the Router 13

4.1 Login 13

4.2 Status 13

4.3 Quick Setup 14

4.4 Network 15

4.4.1 LAN 15

4.4.2 WAN 15

4.4.3 MAC Clone 26

4.5 Wireless 27

4.5.1 Wireless Settings 27

4.5.2 MAC Filtering 32

4.5.3 Wireless Statistics 35

4.6 DHCP 36
4.6.1 DHCP Settings 36
4.6.2 DHCP Clients List 37
4.6.3 Address Reservation 37
4.7 Forwarding 39
4.7.1 Virtual Servers 39
4.7.2 Port Triggering 41
4.7.3 DMZ 43
4.7.4 UPnP 43
4.8 Security 44
4.8.1 Firewall 45
4.8.2 IP Address Filtering 45
4.8.3 Domain Filtering 48
4.8.4 MAC Filtering 49
4.8.5 Remote Management 51
4.8.6 Advanced Security 52
4.9 IP & MAC Binding Setting 54
4.9.1 Binding Setting 54
4.9.2 ARP List 56
4.10 Static Routing 56
4.11 DDNS 58
4.11.1 Dyndns.org DDNS 58
4.11.2 Oray.net DDNS 59
4.11.3 Comexe.cn DDNS 59
4.12 System Tools 60
4.12.1 Time 61
4.12.2 Firmware 62
4.12.3 Factory Defaults 63

4.12.4 Backup and Restore 63
4.12.5 Reboot 64
4.12.6 Password 64
4.12.7 Log 65
4.12.8 Statistics 65
Appendix A: FAQ 68
Appendix B: Configuring the PC 73
Appendix C: Specifications 77
Appendix D: Glossary 78

Chapter 1. Introduction

Thank you for choosing TL-WR541G 54Mbps Wireless Router.

1.1 Overview of the Router

The TL-WR541G 54Mbps Wireless Router integrates 4-port Switch, Firewall, NAT-router and Wireless AP. Its design is dedicated to Small Office/Home Office (SOHO) wireless network solutions. The TL-WR541G 54Mbps Wireless Router will allow you to connect your network wirelessly better than ever, sharing Internet Access, files and fun, easily and securely.

In the most attentive wireless security, the TL-WR541G 54Mbps Wireless Router provides multiple protection measures. It can be set to turn off wireless network name (SSID) broadcast so that only stations that have the SSID can be connected. The router provides wireless LAN 64/128/152-bit WEP encryption security, and WPA/WPA2 and WPA-PSK/WPA2-PSK authentication, as well as TKIP/AES encryption security. It also supports VPN pass-through for sensitive data secure transmission.

The TL-WR541G 54Mbps Wireless Router complies with the IEEE 802.11g and IEEE 802.11b standards so that the data transmission rate is up to 54Mbps. It adopts **2x to 3x eXtended Range™ WLAN transmission technology** so that transmission distance is 2-3 times of traditional IEEE 802.11g and IEEE 802.11b solutions, up to a distance of 855.36m tested in China. Transmission range is extended to 4-9 times. It is compatible with all IEEE 802.11g and IEEE 802.11b products.

The TL-WR541G 54Mbps Wireless Router provides flexible access control so that parents or network administrators can establish restricted access policies for children or staff. It has built-in NAT and DHCP server supporting static IP address distributing. It also supports Virtual Server and DMZ host for Port Triggering needs, and remote management and log so that network administrators can manage and monitor the network in real time. This device supports Bridge mode which can make two APs communicate with each other wirelessly.

The TL-WR541G 54Mbps Wireless Router is easy-to-manage. Quick Setup is supported and friendly help messages are provided for every step. So you can configure it quickly and share Internet access, files and fun.

1.2 Features

- Complies with IEEE 802.11g, IEEE 802.11b, IEEE 802.3, IEEE 802.3u standards.
- 1 10/100M Auto-Negotiation RJ45 WAN port, 4 10/100M Auto-Negotiation RJ45 LAN ports,

supporting Auto MDI/MDIX.

- Adopts 2x to 3x eXtended Range™ wireless LAN transmission technology.
- Supports 54/48/36/24/18/12/9/6Mbps or 11/5.5/3/2/1Mbps data transfer rates.
- Provides WPA/WPA2, WPA-PSK/WPA2-PSK authentication, TKIP/AES encryption security.
- Shares data and Internet access for users, supporting PPPoE, Dynamic IP, Static IP, L2TP, PPTP, BigPond Cable Internet access.
- Supports Virtual Server, Special Application and DMZ host.
- Supports UPnP, Dynamic DNS, Static Routing, VPN Pass-through.
- Connecting Internet on demand and disconnecting from the Internet when idle for PPPoE.
- Built-in NAT and DHCP server supporting static IP address distributing.
- Built-in firewall supporting IP address filtering, Domain Name filtering, and MAC address filtering.
- Supports connecting/disconnecting from the Internet on a specified time of day.
- Supports access control, parents and network administrators can establish restricted access policies based on time of day for children or staff.
- Provides 64/128/152-bit WEP encryption security and wireless LAN ACL (Access Control List).
- Supports Flow Statistics.
- Supports ICMP-FLOOD, UDP-FLOOD, and TCP-SYN-FLOOD filter.
- Ignores Ping packets from WAN or LAN ports.
- Supports firmware upgrade.
- Supports Web management.

1.3 Panel Layout

1.3.1 The Front Panel

The Router's LEDs are located on the front panel (View from left to right).



Figure 1-1 Front Panel sketch

Name	Status	Indication
PWR	Off	Power off
	On	Power on
SYS	On	The router is initializing or maybe has a system error.
	Flashing	The router is working properly
	Off	The router has a hardware error
WLAN	Off	There is no wireless device linked to the router
	Flashing	The Wireless function is enabled
WAN,1-4	Off	There is no device linked to the corresponding port
	On	There is a device linked to the corresponding port but no activity
	Flashing	There is an active device linked to the corresponding port

Table 2-1 The LEDs description

1.3.2 The Rear Panel

The following parts are located on the rear panel (View from left to right).

- **AC power socket**: Please use the power adapter which is supplied with the TL-WR541G 54Mbps Wireless Router only, the use of a different adapter may result in product damage.
- **LAN 1,2,3,4:** Four 10/100Mbps RJ45 LAN ports for connecting the router to the local PC(s)
- **WAN:** This WAN port is where you will connect the cable/DSL Modem, or Ethernet
- **Reset button:**

  There are two ways to reset the router's factory defaults:

  1) Use the **Factory Defaults** function on **System Tools** -> **Factory Defaults** page in the router's Web-based Utility.

  2) Use the Factory Default Reset button: First, turn off the router's power. Second, press and hold the default reset button then turn on the router's power, until the SYS LED lights up (about 3 seconds). Last, release the reset button and wait for the router to reboot.

  ☞ **Note:** Ensure the router is powered on before it restarts completely.

- **Wireless antenna**

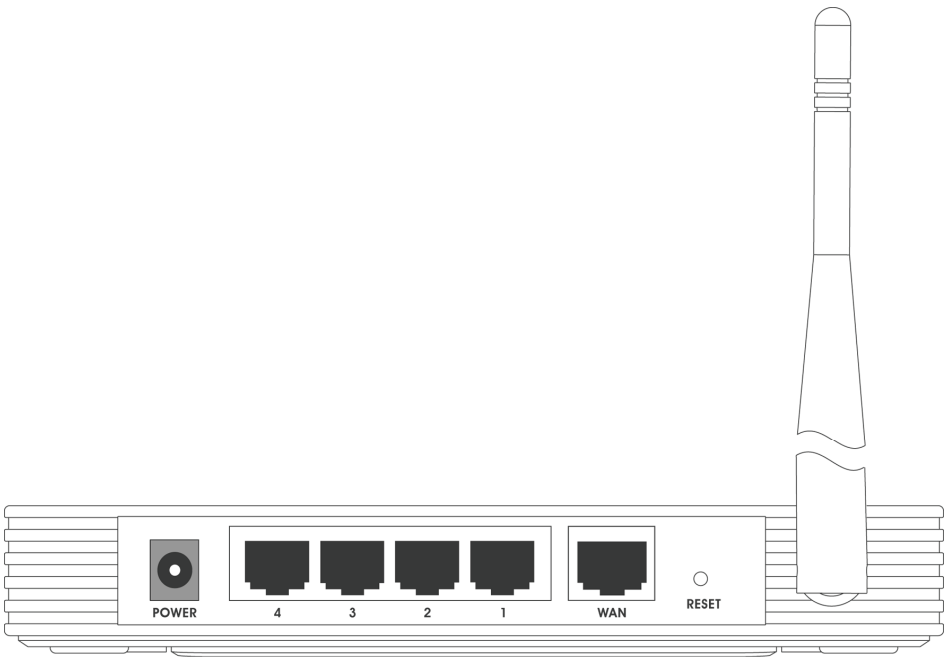


Figure 1-2 Rear Panel sketch

Chapter 2. Connecting the Router

2.1 System Requirements

- Broadband Internet Access Service (DSL/Cable/Ethernet)
- One DSL/Cable Modem that has an RJ45 connector (you do not need it if you connect the router to the Ethernet)
- Each PC in the LAN needs a working Ethernet Adapter and an Ethernet cable with RJ45 connectors
- TCP/IP protocol must be installed on each PC
- Web browser, such as Microsoft Internet Explorer 5.0 or later, Netscape Navigator 6.0 or later

2.2 Installation Environment Requirements

- Do not place in direct sunlight or near a heater or heating vent
- Do not cluttered or crowded. There should be at least 2 inches (5 cm) of clear space on all sides of the router
- Well ventilated (especially if it is in a closet)
- Operating temperature: 0℃~40℃ (32℉~104℉)
- Operating Humidity: 10%~90%RH, Non-condensing

2.3 Connecting the Router

Before you install the router, you should connect your PC to the Internet through your broadband service successfully. If there is any problem, please contact your ISP. After that, please install the router according to the following steps. Don't forget to pull out the power plug and keep your hands dry.

1. Power off your PC, Cable/DSL Modem, and the router.
2. Locate an optimum location for the router. The best place is usually near the center of the area in which your PC will connect wirelessly. The place must accord with the Installation Environment Requirements.
3. Adjust the direction of the antenna. Normally, upright is a good direction.
4. Connect the PC(s) and each Switch/Hub in your LAN to the LAN Ports on the router, shown in Figure 2-1. (If you have the wireless NIC and want to use wireless function, you can skip this

step.)

5. Connect the DSL/Cable Modem to the WAN port on the router, shown in Figure 2-1.

6. Connect the AC power adapter to the AC power socket on the router, and the other end into an electrical outlet. The router will start to work automatically.

7. Power on your PC and Cable/DSL Modem.

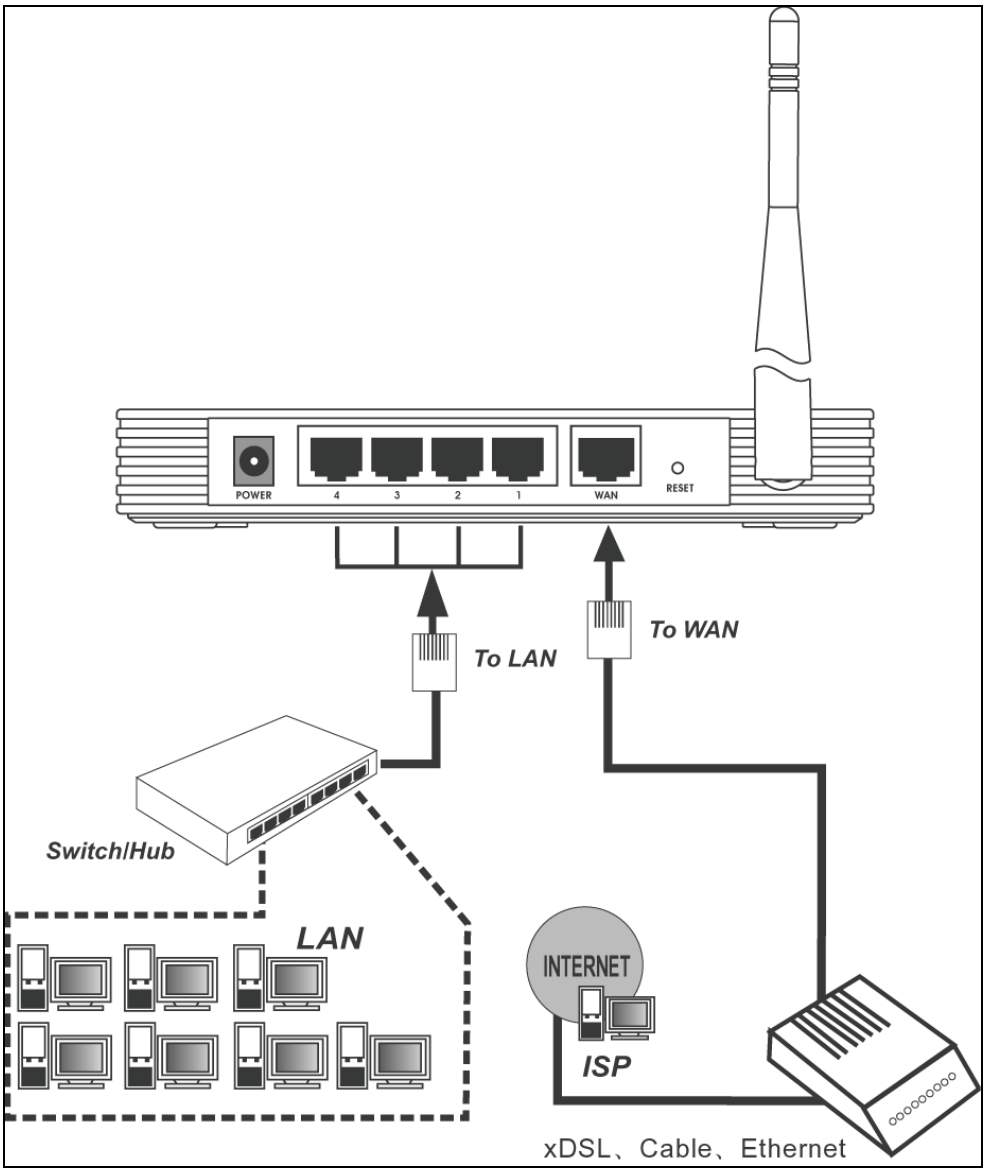


Figure 2-1 Hardware Installation of the TL-WR541G 54Mbps Wireless Router

Chapter 3. Quick Installation Guide

After connecting the TL-WR541G Router into your network, you should configure it. This chapter describes how to configure the basic functions of your TL-WR541G Wireless Router. These procedures only take you a few minutes. You can access the Internet via the router immediately after successfully configuring.

3.1 TCP/IP configuration

The default IP address of the TL-WR541G 54Mbps Wireless Router is 192.168.1.1. And the default Subnet Mask is 255.255.255.0. These values can be seen from the LAN. They can be changed as you desire, as an example we use the default values for description in this guide.

Connect the local PC to the LAN ports of the router. There are then two ways to configure the IP address for your PC.

- Configure the IP address manually

  1) Set up the TCP/IP Protocol for your PC. If you need instructions as to how to do this, please refer to Appendix B: "Configuring the PC."

  2) Configure the network parameters. The IP address is 192.168.1.xxx ("xxx" is from 2 to 254), Subnet Mask is 255.255.255.0, and Gateway is 192.168.1.1 (The router's default IP address)

- Obtain an IP address automatically

  1) Set up the TCP/IP Protocol in "**Obtain an IP address automatically**" mode on your PC. If you need instructions as to how to do this, please refer to Appendix B: "Configuring the PC."

  2) Power off the router and PC. Then turn on the router and restart the PC. The built-in DHCP server will assign IP address for the PC.

☞ **Note:** For Windows 98 OS or earlier, the PC and router may need to be restarted.

Now, you can run the Ping command in the **command prompt** to verify the network connection between your PC and the router. The following example is in Windows 2000 OS.

Open a command prompt, and type *ping 192.168.1.1*, and then press **Enter**.

If the result displayed is similar to that shown in Figure 3-1, the connection between your PC and the router has been established.

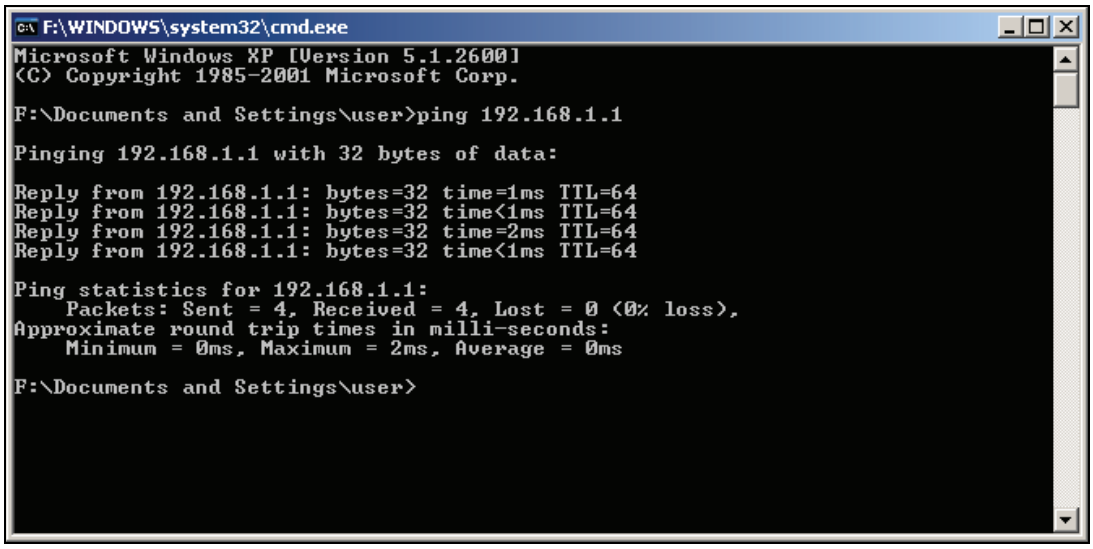


Figure 3-1 Success result of Ping command

If the result displayed is similar to that shown in Figure 3-2, it means that your PC has not connected to the router.

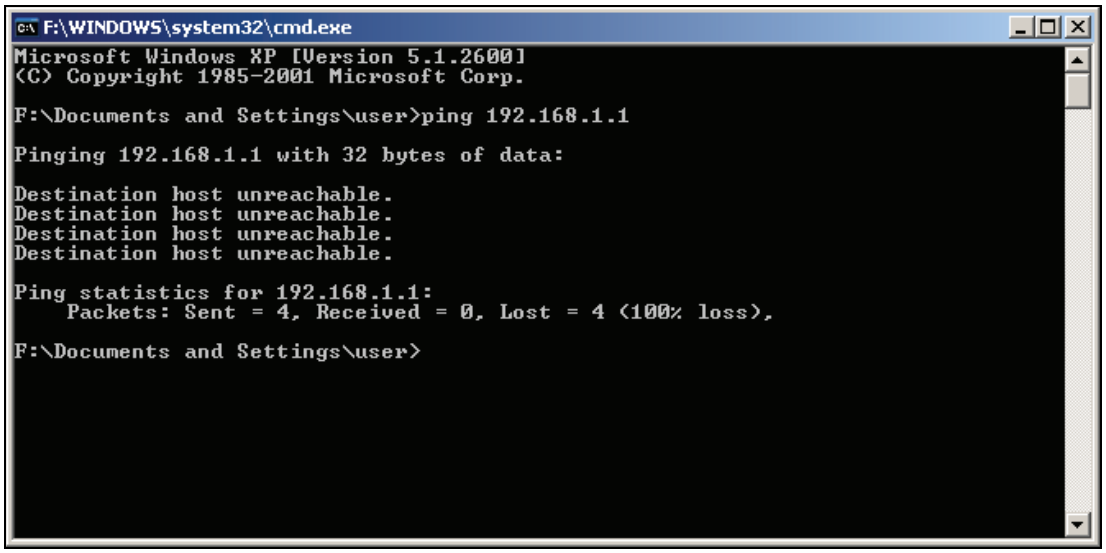


Figure 3-2 Failure result of Ping command

Please check the connection following these steps:

1. Is the connection between your PC and the router correct?

☞ **Note:**

The 1/2/3/4 LEDs of LAN port which you link to on the router and LEDs on your PC's adapter should be lit.

2. Is the TCP/IP configuration for your PC correct?

☞ **Note:**

If the router's IP address is 192.168.1.1, your PC's IP address must be within the range of 192.168.1.2 ~ 192.168.1.254, the gateway must be 192.168.1.1

3.2 Quick Installation Guide

With a Web-based (Internet Explorer or Netscape® Navigator) utility, it is easy to configure and manage the TL-WR541G 54Mbps Wireless Router. The Web-based utility can be used on any Windows, Macintosh or UNIX OS with a Web browser.

Connect to the router by typing *http://192.168.1.1* in the address field of Web browser.



Figure 3-3 Login the router

After a moment, a login window will appear similar to that shown in Figure 3-4. Enter **admin** for the User Name and Password, both in lower case letters. Then click the **OK** button or press the **Enter** key.



Figure 3-4 Login Windows

☞ **Note:**

If the above screen does not pop-up, it means that your Web-browser has been set to a proxy. Go to Tools menu>Internet Options>Connections>LAN Settings, in the screen that appears, cancel the Using Proxy checkbox, and click OK to finish it.

If the User Name and Password are correct, you can configure the router using the Web browser. Please click the **Quick Setup** link on the left of the main menu and the Quick Setup screen will appear.

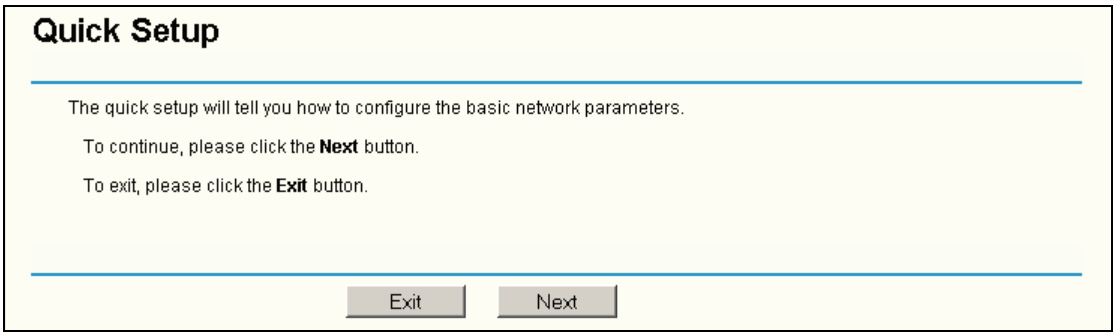


Figure 3-5 Quick Setup

Click **Next**, and then **Choose WAN Connection Type** page will appear, shown in Figure 3-6.

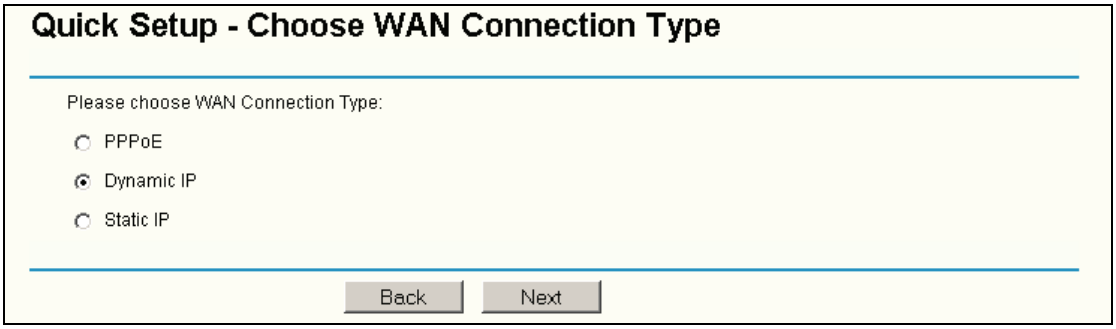


Figure 3-6 Choose WAN Connection Type

The router supports three popular ways to connect to Internet. Please select one compatible with your ISP. Click Next to enter the necessary network parameters.

If you choose "PPPoE", you will see this page shown in Figure 3-7:

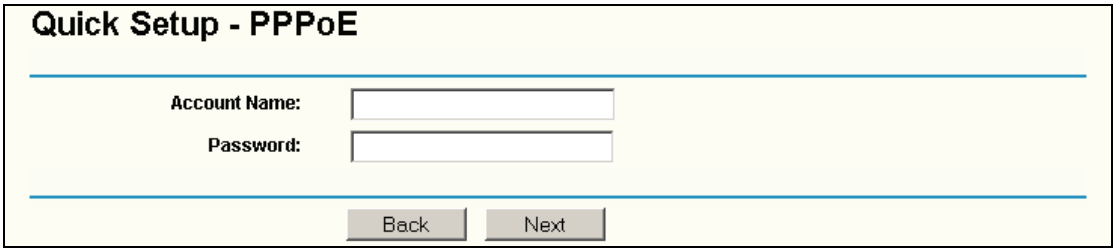


Figure 3-7 Quick Setup - PPPoE

- **Account Name** and **Password -** Enter the **Account Name** and **Password** provided by your ISP. These fields are case sensitive. If you have difficulty with this process, please contact your ISP.

If you choose "**Dynamic IP**", the router will automatically receive the IP parameters from your ISP without needing to enter any parameters.

If you Choose "**Static IP**", the Static IP settings page will appear, shown in Figure 3-8:

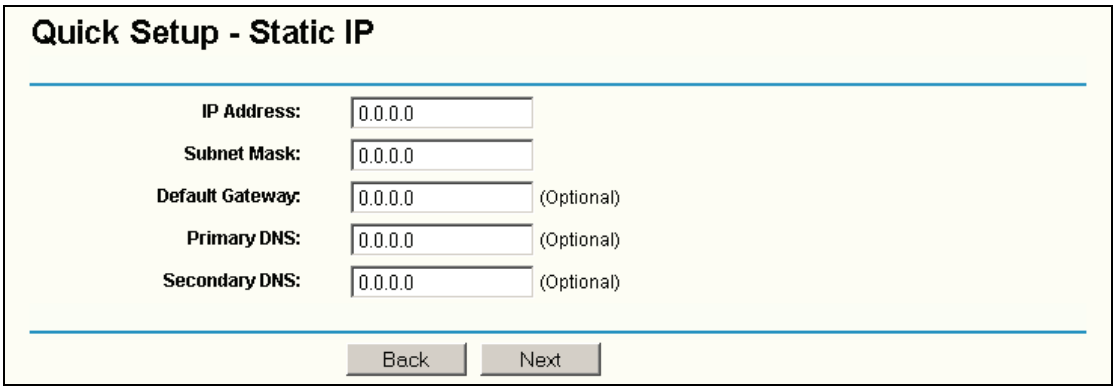


Figure 3-8 Quick Setup - Static IP

Note - The IP parameters should have been provided by your ISP.

- **IP Address -** This is the WAN IP address as seen by external users on the Internet (including your ISP). Enter the IP address into the field.
- **Subnet Mask -** The Subnet Mask is used for the WAN IP address, it is usually 255.255.255.0
- **Default Gateway -** Enter the gateway IP address into the box if required.
- **Primary DNS -** Enter the DNS Server IP address into the boxes if required.
- **Secondary DNS -** If your ISP provides another DNS server, enter it into this field.

After you complete the above, click **Next**, the Wireless settings page will appear, shown in Figure 3-9.

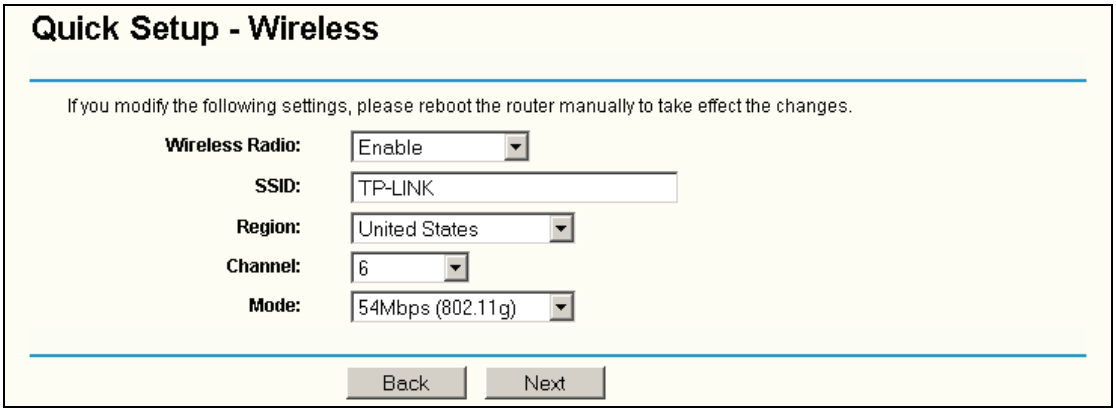


Figure 3-9 Quick Setup - Wireless settings

In this page, you can configure the following wireless parameters:

- **Wireless Radio -** Indicates whether the Access Point feature of the router is enabled or disabled. If disabled, the WLAN LED on the front panel will not be lit and the wireless stations will not be able to access the router. If enabled, the WLAN LED will be lit up and wireless stations will be able to access the router.
- **SSID -** Enter a value of up to 32 characters. The same SSID must be assigned to all

wireless devices on your network. The default SSID is TP-LINK. This value is case-sensitive. For example, *TP-LINK* is NOT the same as *tp-link*.

- **Region -** Select your region from the pull-down list. This field specifies the region where the wireless function of the router can be used. It may be illegal to use the wireless function of the router in a region other than one of those specified in this field.
- **Channel -** The current channel in use. This field determines which operating frequency will be used.
- **Mode -** Indicates the current mode **54Mbps (802.11g)**, **11Mbps (802.11b)**. If you select **54Mbps (802.11g)**, it is compatible with **11Mbps (802.11b)**.

These settings are only for basic wireless parameters, for advanced settings, please refer to Section 4.5: "Wireless."

☞ **Note:**

The change of wireless settings won't take effect until the router reboots! You can reboot it manually. If you need instructions as to how to do this, please refer to Section 4.12.5: "Reboot".

Click the **Next** button. You will then see the Finish page:

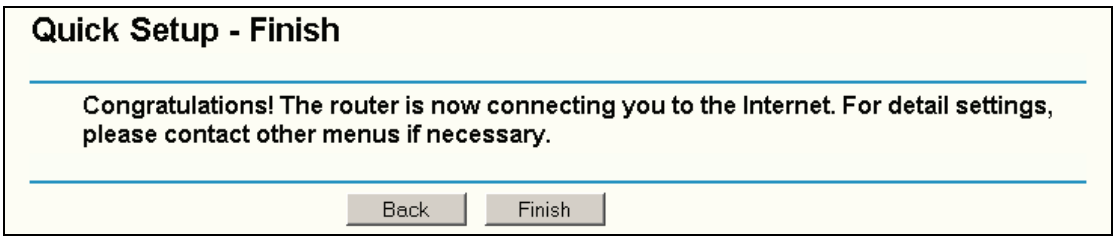


Figure 3-10 Quick Setup - Finish

After finishing all configurations of basic network parameters, please click **Finish** button to exit this **Quick Setup**.

Chapter 4. Configuring the Router

This chapter describes each Web page's key functions.

4.1 Login

After your successful login, you can configure and manage the router. There are ten main menus on the left of the Web-based utility. Submenus will be available after you click one of the main menus. The eleven main menus are: **Status, Quick Setup, Network, Wireless, DHCP, Forwarding, Security, IP & MAC Binding Setting, Static Routing, DDNS and System Tools.** On the right of the Web-based utility, there are the detailed explanations and instructions for the corresponding page. To apply any settings you have altered on the page, please click the **Save** button.

The detailed explanations for each Web page key's function are listed below.

4.2 Status

The Status page displays the router's current status and configuration. All information is read-only.

1. **LAN**

   This field displays the current settings or information for the LAN, including the **MAC address, IP address and Subnet Mask.**

2. **Wireless**

   This field displays basic information or status for wireless function, including **Wireless Radio, SSID, Channel, Mode, Wireless MAC address, and IP address.**

3. **WAN**

   These parameters apply to the WAN port of the router, including **MAC address, IP address, Subnet Mask, Default Gateway, DNS server** and **WAN connection type**. If PPPoE is chosen as the WAN connection type, the **Disconnect** button will be shown here while you are accessing the Internet. You can also cut the connection by clicking the button. If you have not connected to the Internet, just click **Connect** to establish the connection.

4. **Traffic Statistics**

   This field displays the router's traffic statistics.

5. **System Up Time**

The total up time of the router from when it was switched on or reset.

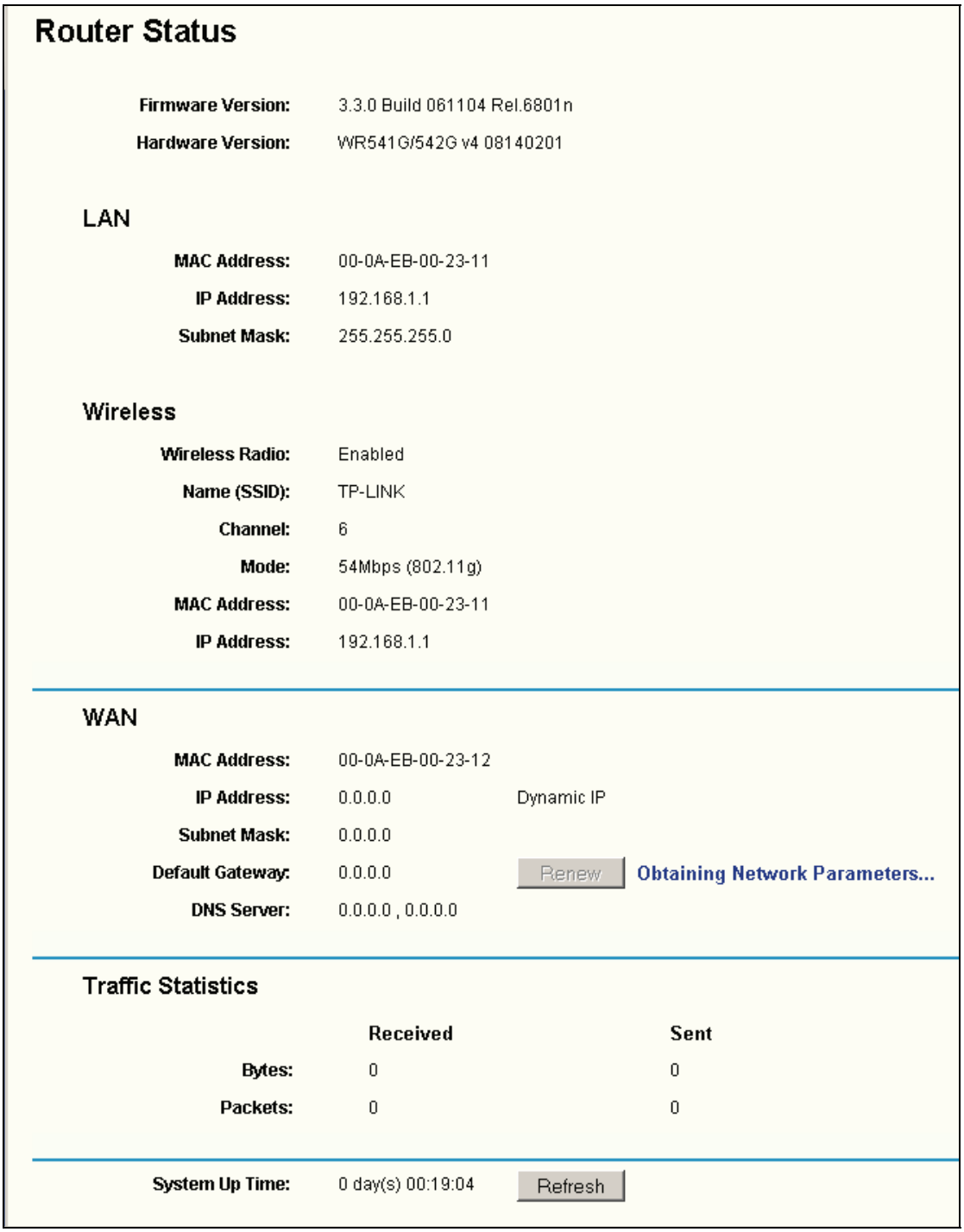


Figure 4-1 Router Status

4.3 Quick Setup

Please refer to Section 3.2: "Quick Installation Guide."

4.4 Network



Figure 4-2 the Network menu

There are three submenus under the Network menu (shown in Figure 4-2): **LAN**, **WAN** and **MAC Clone.** Click any of them, and you will be able to configure the corresponding function. The detailed explanations for each submenu are provided below.

4.4.1 LAN

You can configure the IP parameters of LAN on this page.

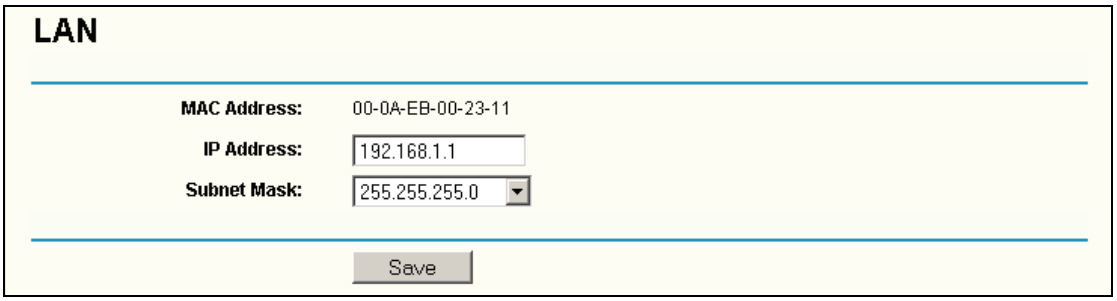


Figure 4-3 LAN

- **MAC Address -** The physical address of the router, as seen from the LAN. The value can't be changed.
- **IP Address -** Enter the IP address of your router in dotted-decimal notation (factory default: 192.168.1.1).
- **Subnet Mask -** An address code that determines the size of the network. Normally use 255.255.255.0 as the subnet mask.

☞ **Note:**

a. If you change the IP Address of LAN, you must use the new IP Address to login the router.

b. If the new LAN IP Address you set is not in the same subnet, the IP Address pool of the DHCP server will not take effect, until they are re-configured.

c. If the new LAN IP Address you set is not in the same subnet, the Virtual Server and DMZ Host will change accordingly at the same time.

4.4.2 WAN

You can configure the WAN port parameters on this page.

First, please choose the WAN Connection Type (Dynamic IP/Static IP/PPPoE/802.1X + Dynamic IP/802.1X + Static IP/Big Pond Cable/L2TP/PPTP) for Internet. The default type is **Dynamic IP**. If you aren't given any login parameters (fixed IP Address, logging ID, etc), please select **Dynamic IP**. If you are given a fixed IP (static IP), please select **Static IP**. If you are given a user name and a password, please select the type of your ISP provided (PPPoE/BigPond/L2TP/PPTP). If you are not sure which connection type you use currently, please contact your ISP to obtain the correct information.

1. If you choose **Dynamic IP,** the router will automatically get IP parameters from your ISP. You can see the page as follows (Figure 4-4):

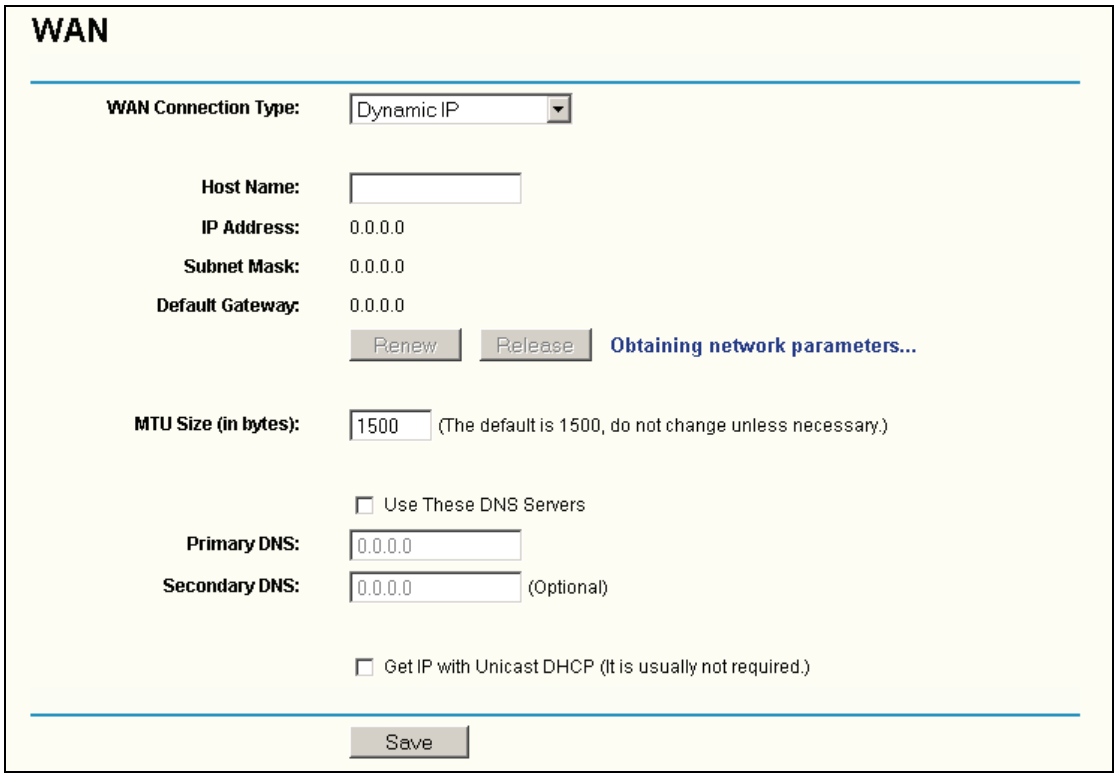


Figure 4-4 WAN – Dynamic IP

This page displays the WAN IP parameters assigned dynamically by your ISP, including IP address, Subnet Mask, Default Gateway, etc. Click the **Renew** button to renew the IP parameters from your ISP. Click the **Release** button to release the IP parameters.

MTU Size - The normal MTU (Maximum Transmission Unit) value for most Ethernet networks is 1500 Bytes. For some ISPs you need to reduce the MTU. But this is rarely required, and should not be done unless you are sure it is necessary for your ISP connection.

If your ISP gives you one or two DNS addresses, select **Use These DNS Servers** and enter the primary and secondary addresses into the correct fields. Otherwise, the DNS servers will be assigned dynamically from your ISP.

☞ **Note:**

If you get address and find error when you go to a Web site, it is likely that your DNS servers are set up improperly. You should contact your ISP to get DNS server addresses.

Get IP with Unicast DHCP - A few ISPs' DHCP servers do not support the broadcast applications. If you cannot get the IP Address normally, you can choose this option. (This is rarely required.)

2. If you choose **Static IP,** you should have fixed IP Parameters specified by your ISP. The Static IP settings page will appear, shown in Figure 4-5:

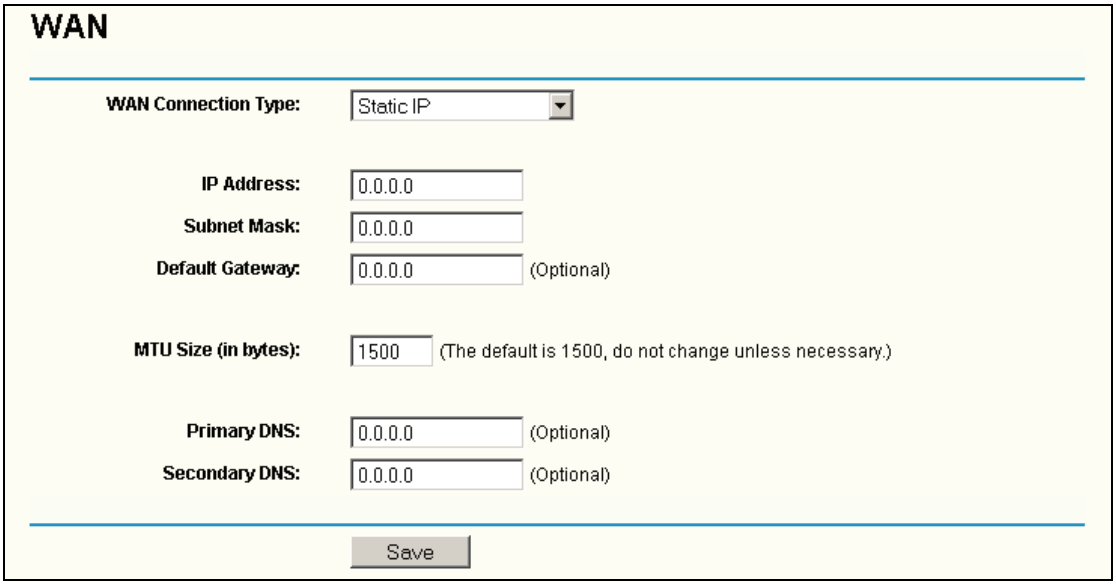


Figure 4-5 WAN - Static IP

You should type the following parameters into the spaces provided:

- **IP Address -** Enter the IP address in dotted-decimal notation provided by your ISP.
- **Subnet Mask -** Enter the subnet Mask in dotted-decimal notation provided by your ISP, usually is 255.255.255.0.
- **Default Gateway -** (Optional) Enter the gateway IP address in dotted-decimal notation provided by your ISP.
- **MTU Size -** The normal MTU (Maximum Transmission Unit) value for most Ethernet networks is 1500 Bytes. For some ISPs you may need to modify the MTU. But this is rarely required, and should not be done unless you are sure it is necessary for your ISP connection.
- **Primary DNS -** (Optional) Enter the DNS address in dotted-decimal notation provided by your ISP.
- **Secondary DNS -** (Optional) Type another DNS address in dotted-decimal notation provided by your ISP if provided.

3. If you choose **PPPoE,** you should enter the following parameters (Figure 4-6):

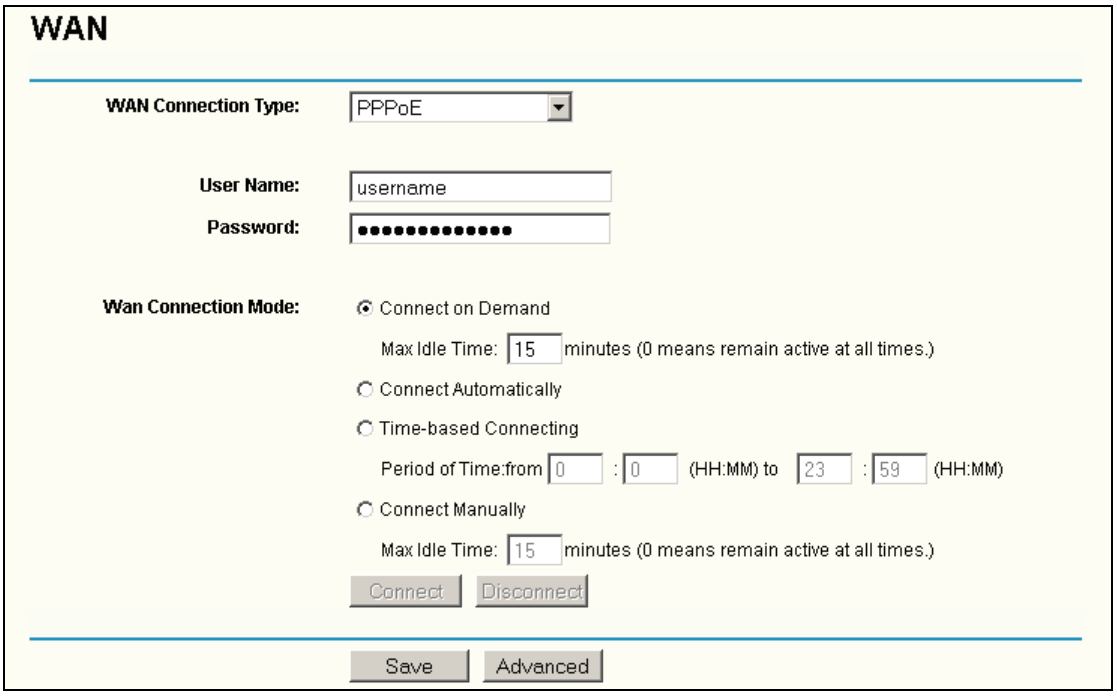


Figure 4-6 WAN - PPPoE

- **User Name/Password -** Enter the User Name and Password provided by your ISP. These fields are case-sensitive.

- **Connect on Demand -** You can configure the router to disconnect your Internet connection after a specified period of inactivity (**Max Idle Time**). If your Internet connection has been terminated due to inactivity, **Connect on Demand** enables the router to automatically re-establish your connection as soon as you attempt to access the Internet again. If you wish to activate **Connect on Demand**, click the radio button. If you want your Internet connection to remain active at all times, enter 0 in the **Max Idle Time** field. Otherwise, enter the number of minutes you want to have elapsed before your Internet connection terminates.

  Caution: Sometimes the connection cannot be disconnected although you specify a time to Max Idle Time, since some applications is visiting the Internet continually in the background.

- **Connect Automatically -** Connect automatically after the router is disconnected. To use this option, click the radio button.

- **Time-based Connecting -** You can configure the router to make it connect or disconnect based on time. Enter the start time in HH:MM format for connecting and end time in HH:MM format for disconnecting in the **Period of Time** fields.

  Note:

  Only when you have configured the system time on **System Tools -> Time** page, will the **Time-based Connecting** function can take effect.

- **Connect Manually -** You can configure the router to make it connect or disconnect manually. After a specified period of inactivity (**Max Idle Time**), the router will disconnect from the Internet connection, and you will not be able to re-establish your connection automatically as soon as you attempt to access the Internet again. To use this option, click the radio button. If you want your Internet connection to remain active at all times, enter "0" in the **Max Idle Time** field. Otherwise, enter the number time in minutes that you wish to have the Internet connecting last unless a new link is requested.

Caution: Sometimes the connection cannot be disconnected although you specify a time to Max Idle Time, since some applications are visiting the Internet continually in the background.

Click the **Connect** button to connect immediately. Click the **Disconnect** button to disconnect immediately.

Click the **Advanced Settings** button to set up the advanced option, the page shown in Figure 4-7 will then appear:

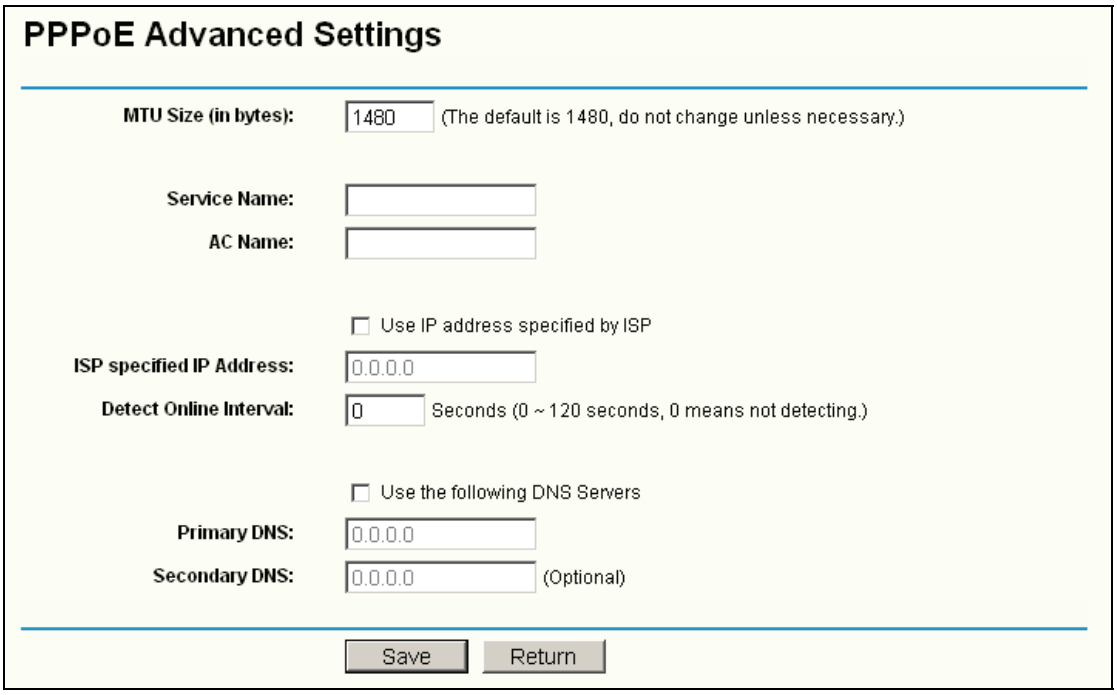


Figure 4-7 PPPoE Advanced Settings

- **Packet MTU -** The default MTU size is 1480 bytes, which value is usually fine. For some ISPs, you need modify the MTU. This should not be done unless you are sure it is necessary for your ISP.
- **Service Name/AC Name -** The service name and AC (Access Concentrator) name, these should not be configured unless you are sure it is necessary for your ISP.
- **ISP Specified IP Address -** If you know that your ISP does not automatically transmit your IP address to the router during login, click "**Use the IP Address specified by ISP**" check box

and enter the IP Address in dotted-decimal notation, which your ISP provided.

- **Detect Online Interval -** The default value is 0, you can input the value between 0 and 120. The router will detect Access Concentrator online at every interval between seconds. If the value is 0, it means, do not detect.
- **DNS IP address -** If you know that your ISP does not automatically transmit DNS addresses to the router during login, click "**Use the following DNS servers**" checkbox and enter the IP address in dotted-decimal notation of your ISP's primary DNS server. If a secondary DNS server address is available, enter it as well.

Click the **Save** button to save your settings.

4. If you choose **802.1X + Dynamic IP,** you should enter the follow parameters(Figure 4-8) :

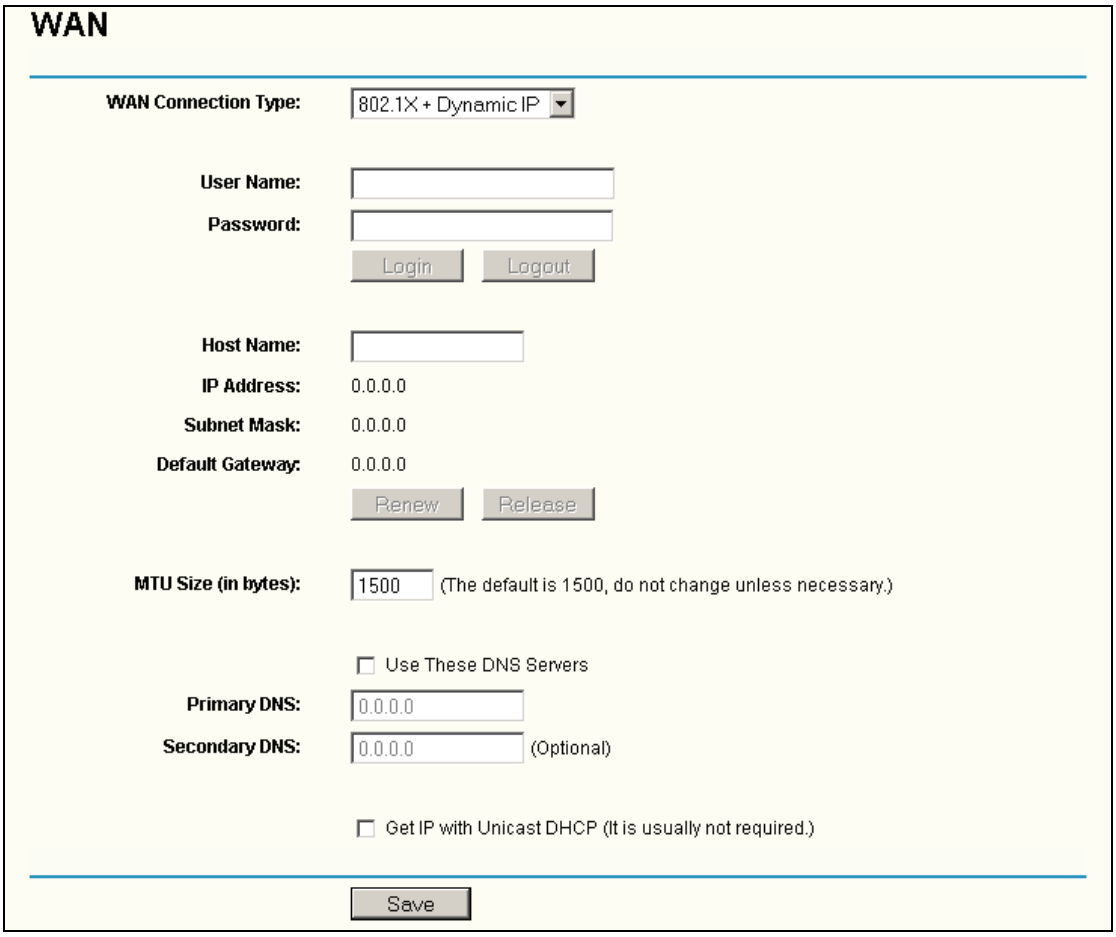


Figure 4-8 802.1X + Dynamic IP Settings

- **User Name -** Enter the user name for 802.1X authentication provided by your ISP
- **Password -** Enter the password for 802.1X authentication provided by your ISP.

Click **Login** to start 802.1X authentication.

Click **Logout** to end 802.1X authentication.

- **Host Name** - This field is required to be filled by some service provider.

5. If you choose **802.1X + Static IP,** you should enter the follow parameters(Figure 4-9) :

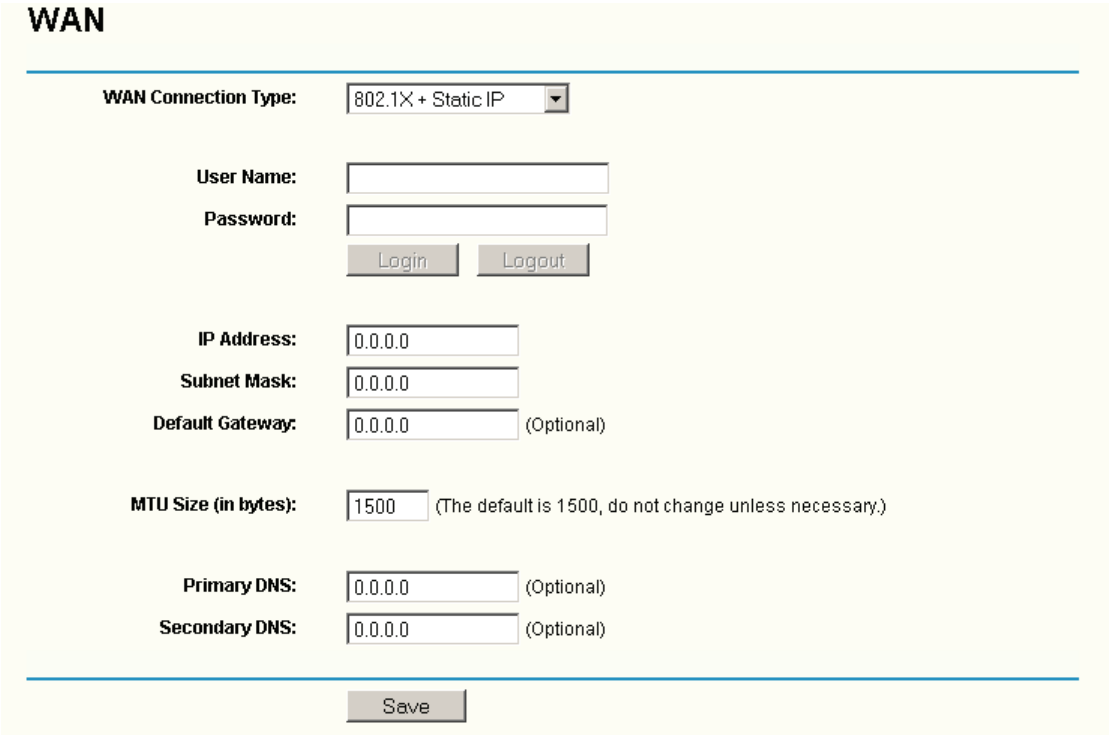


Figure 4-9 802.1X + Static IP Settings

- **User Name -** Enter the user name for 802.1X authentication provided by your ISP
- **Password -** Enter the password for 802.1X authentication provided by your ISP.

Click **Login** to start 802.1X authentication.

Click **Logout** to end 802.1X authentication.

- **IP Address** - Enter the IP address in dotted-decimal notation provided by your ISP.
- **Subnet Mask** - Enter the subnet Mask in dotted-decimal notation provided by your ISP.
- **Default Gateway** - (Optional) Enter the default gateway IP address in dotted-decimal notation provided by your ISP.

6. If you choose **Big Pond Cable,** you should enter the following parameters (Figure 4-10):

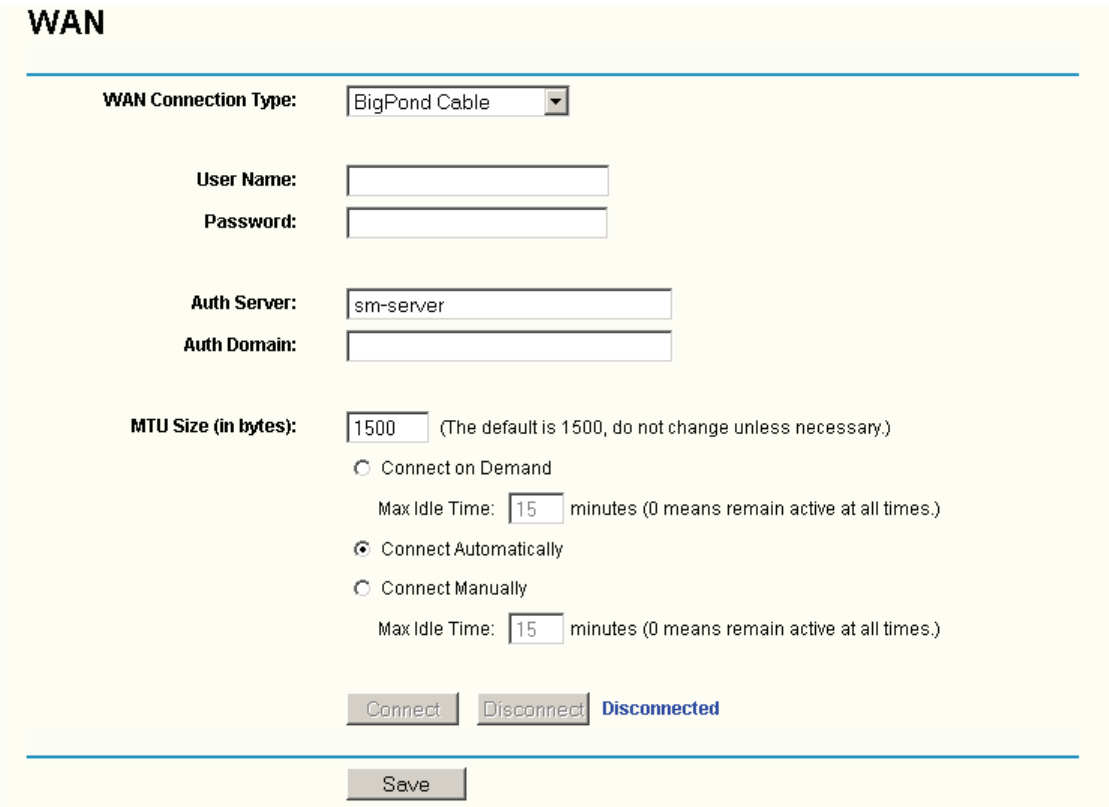


Figure 4-10 Big Pond Settings

- **User Name/Password -** Enter the User Name and Password provided by your ISP. These fields are case-sensitive.
- **Auth Server -** Enter the authenticating server IP address or host name.
- **Auth Domain** - Type in the domain suffix server name based on your location. Egg,
  NSW / ACT - **nsw.bigpond.net.au**
  VIC / TAS / WA / SA / NT - **vic.bigpond.net.au**
  QLD - **qld.bigpond.net.au**
- **Connect on Demand -** You can configure the router to disconnect from your Internet connection after a specified period of inactivity (**Max Idle Time**). If your Internet connection has been terminated due to inactivity, **Connect on Demand** enables the router to automatically re-establish your connection as soon as you attempt to access the Internet again. If you wish to activate **Connect on Demand**, click the radio button. If you want your Internet connection to remain active at all times, enter 0 in the **Max Idle Time** field. Otherwise, enter the number of minutes you want to have elapsed before your Internet connection terminates.

  Caution: Sometimes the connection cannot be disconnected although you specify a time to Max Idle Time, since some applications are visiting the Internet continually in the background.
- **Connect Automatically -** Connect automatically after the router is disconnected. To use this

option, click the radio button.

- **Connect Manually -** You can configure the router to make it connect or disconnect manually. After a specified period of inactivity (**Max Idle Time**), the router will disconnect from your Internet connection, and you will not be able to re-establish your connection automatically as soon as you attempt to access the Internet again. To use this option, click the radio button. If you want your Internet connection to remain active at all times, enter "0" in the **Max Idle Time** field. Otherwise, enter the number in minutes that you wish to have the Internet connecting last unless a new link is requested.

Caution: Sometimes the connection cannot be disconnected although you specify a time to Max Idle Time, since some applications are visiting the Internet continually in the background.

Click the **Connect** button to connect immediately. Click the **Disconnect** button to disconnect immediately.

7. If you choose **L2TP**, you should enter the following parameters (Figure 4-11):

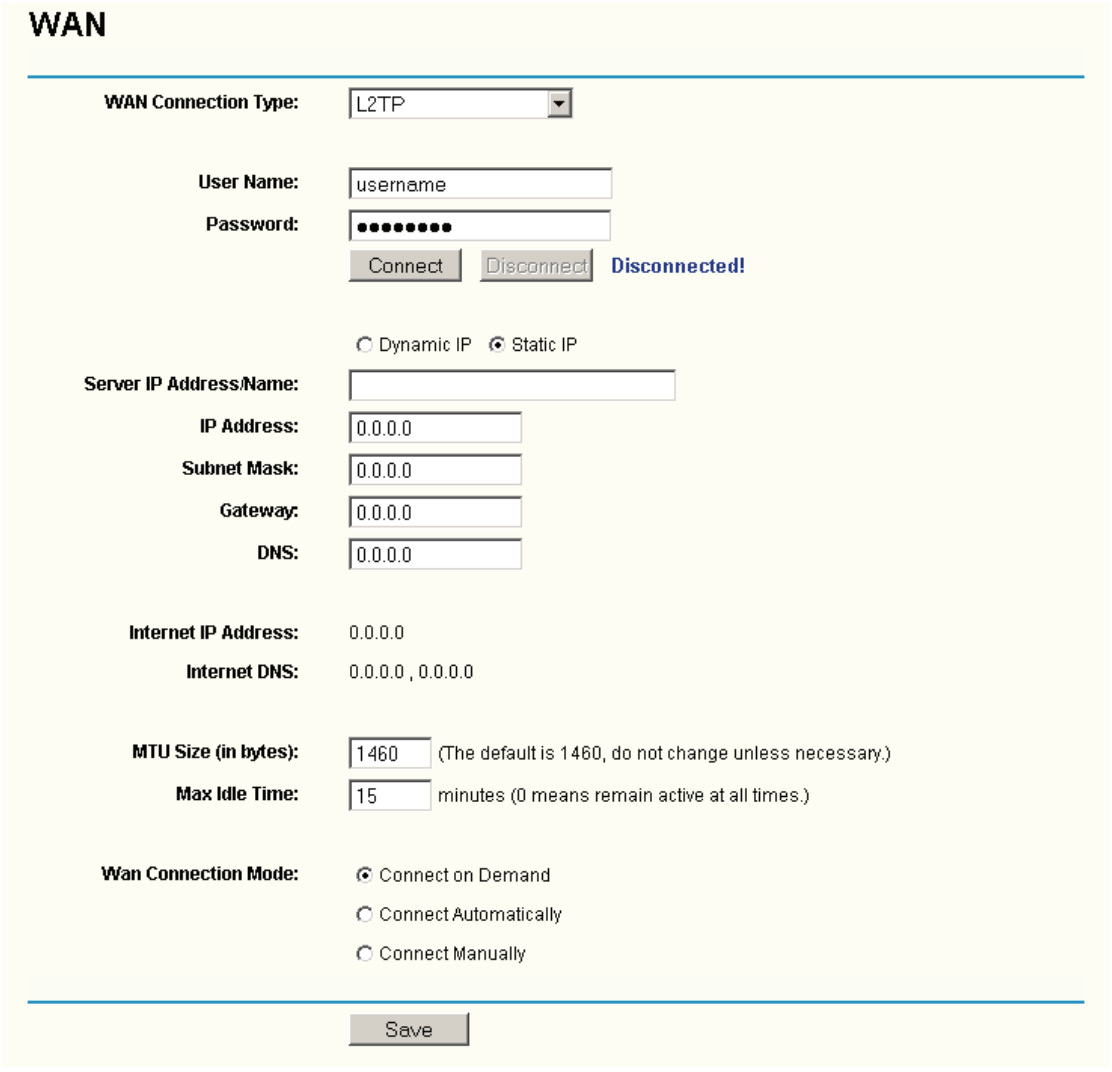


Figure 4-11 L2TP Settings

- **User Name/Password -** Enter the User Name and Password provided by your ISP. These fields are case-sensitive.
- **Dynamic IP/ Static IP –** Choose either as you are given by your ISP.

  Click the **Connect** button to connect immediately. Click the **Disconnect** button to disconnect immediately.
- **Connect on Demand -** You can configure the router to disconnect from your Internet connection after a specified period of inactivity (**Max Idle Time**). If your Internet connection has been terminated due to inactivity, **Connect on Demand** enables the router to automatically re-establish your connection as soon as you attempt to access the Internet again. If you wish to activate **Connect on Demand**, click the radio button. If you want your Internet connection to remain active at all times, enter 0 in the **Max Idle Time** field. Otherwise, enter the number of minutes you want to have elapsed before your Internet connection terminates.

  Caution: Sometimes the connection cannot be disconnected although you specify a time to Max Idle Time, since some applications is visiting the Internet continually in the background.
- **Connect Automatically -** Connect automatically after the router is disconnected. To use this option, click the radio button.
- **Connect Manually -** You can configure the router to make it connect or disconnect manually. After a specified period of inactivity (**Max Idle Time**), the router will disconnect from your Internet connection, and you will not be able to re-establish your connection automatically as soon as you attempt to access the Internet again. To use this option, click the radio button. If you want your Internet connection to remain active at all times, enter "0" in the **Max Idle Time** field. Otherwise, enter the number in minutes that you wish to have the Internet connecting last unless a new link is requested.

  Caution: Sometimes the connection cannot be disconnected although you specify a time to Max Idle Time, since some applications is visiting the Internet continually in the background.

8. If you choose **PPTP**, you should enter the following parameters (Figure 4-12):

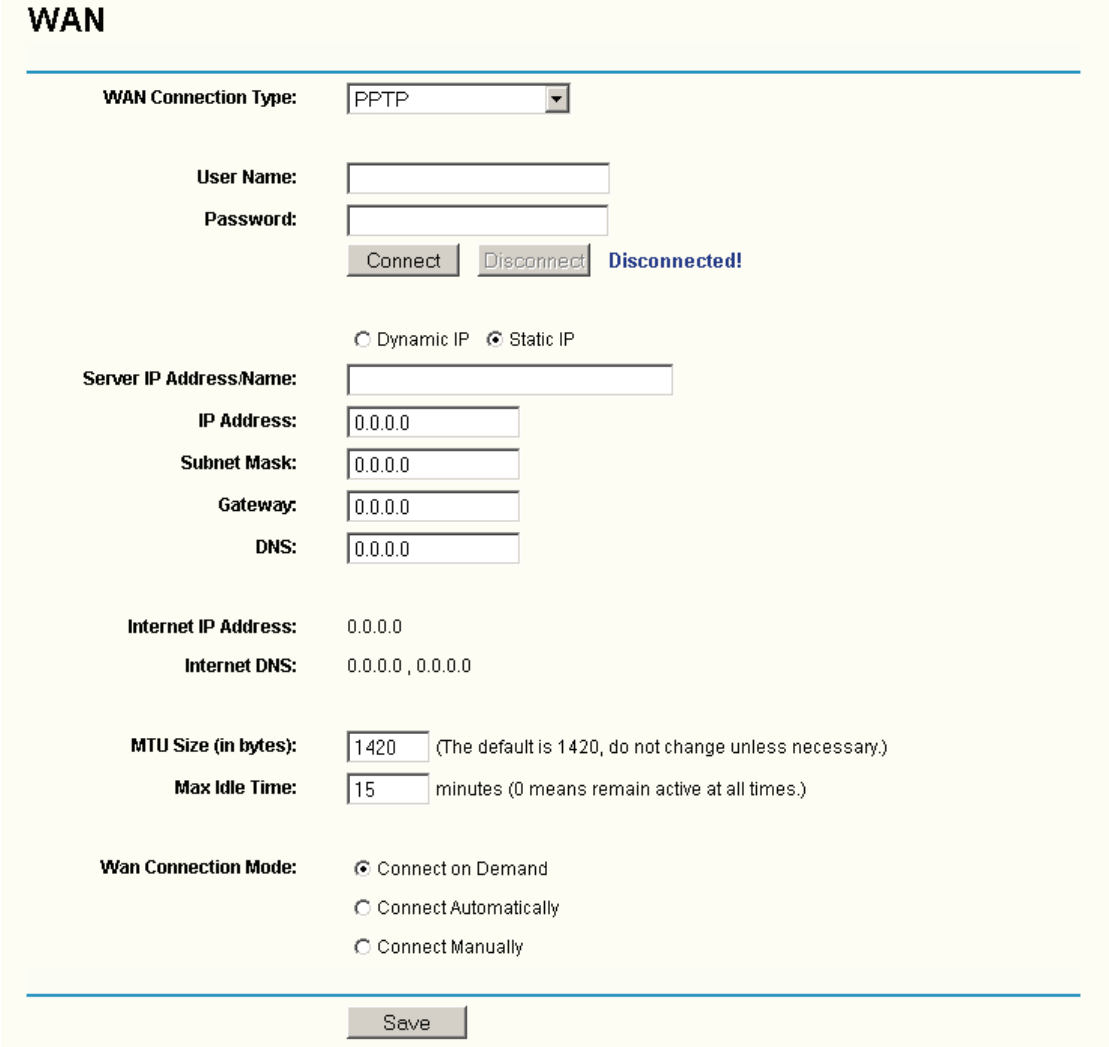


Figure 4-12 PPTP Settings

- **User Name/Password -** Enter the User Name and Password provided by your ISP. These fields are case-sensitive.
- **Dynamic IP/ Static IP –** Choose either as you are given by your ISP and enter the ISP's IP address or the domain name.

  If you choose static IP and enter the domain name, you should also enter the DNS assigned by your ISP. And click the **Save** button.

  Click the **Connect** button to connect immediately. Click the **Disconnect** button to disconnect immediately.
- **Connect on Demand -** You can configure the router to disconnect from your Internet connection after a specified period of inactivity (**Max Idle Time**). If your Internet connection has been terminated due to inactivity, **Connect on Demand** enables the router to automatically re-establish your connection as soon as you attempt to access the Internet again. If you wish to activate **Connect on Demand**, click the radio button. If you want your Internet connection to remain active at all times, enter 0 in the **Max Idle Time** field. Otherwise,

enter the number of minutes you want to have elapsed before your Internet connection terminates.

Caution: Sometimes the connection cannot be disconnected although you specify a time to Max Idle Time, since some applications are visiting the Internet continually in the background.

- **Connect Automatically -** Connect automatically after the router is disconnected. To use this option, click the radio button.
- **Connect Manually -** You can configure the router to make it connect or disconnect manually. After a specified period of inactivity (**Max Idle Time**), the router will disconnect from your Internet connection, and you will not be able to re-establish your connection automatically as soon as you attempt to access the Internet again. To use this option, click the radio button. If you want your Internet connection to remain active at all times, enter "0" in the **Max Idle Time** field. Otherwise, enter the number in minutes that you wish to have the Internet connecting last unless a new link is requested.

Caution: Sometimes the connection cannot be disconnected although you specify a time to Max Idle Time, since some applications are visiting the Internet continually in the background.

4.4.3 MAC Clone

You can configure the MAC address of the WAN port on this page, Figure 4-13:

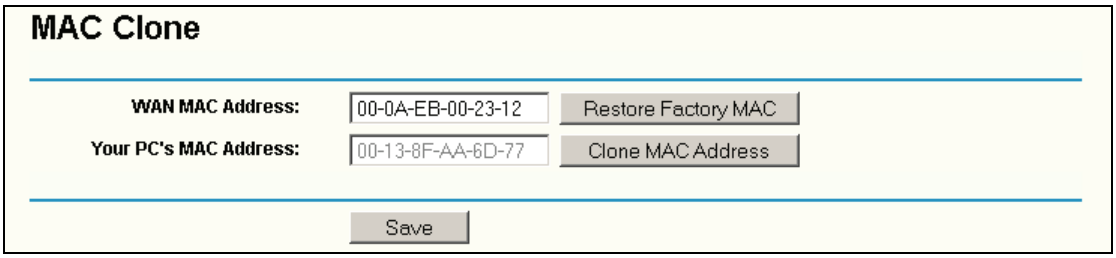


Figure 4-13 MAC Address Clone

Some ISPs require that you register the MAC Address of your adapter, which is connected to your cable/DSL Modem or Ethernet during installation. Changes are rarely needed here.

- **WAN MAC Address -** This field displays the current MAC address of the WAN port, which is used for the WAN port. If your ISP requires that you register the MAC address, please enter the correct MAC address into this field. The format for the MAC Address is XX-XX-XX-XX-XX-XX (X is any hexadecimal digit).
- **Your PC's MAC Address -** This field displays the MAC address of the PC that is managing the router. If the MAC address is required, you can click the **Clone MAC Address** button and this MAC address will fill in the **WAN MAC Address** field.

Click **Restore Factory MAC** to restore the MAC address of WAN port to the factory default value.

Click the **Save** button to save your settings.

☞ **Note:**

1) Only the PC on your LAN can use the **MAC Address Clone** feature.

2) If you click the **Save** button, the router will prompt you to reboot.

4.5 Wireless



Figure 4-14 Wireless menu

There are three submenus under the Wireless menu (shown in Figure 4-14): **Wireless Settings**, **MAC Filtering** and **Wireless Statistics.** Click any of them, and you will be able to configure the corresponding function. The detailed explanations for each submenu are provided below.

4.5.1 Wireless Settings

The basic settings for the wireless network are set on this page, Figure 4-15:

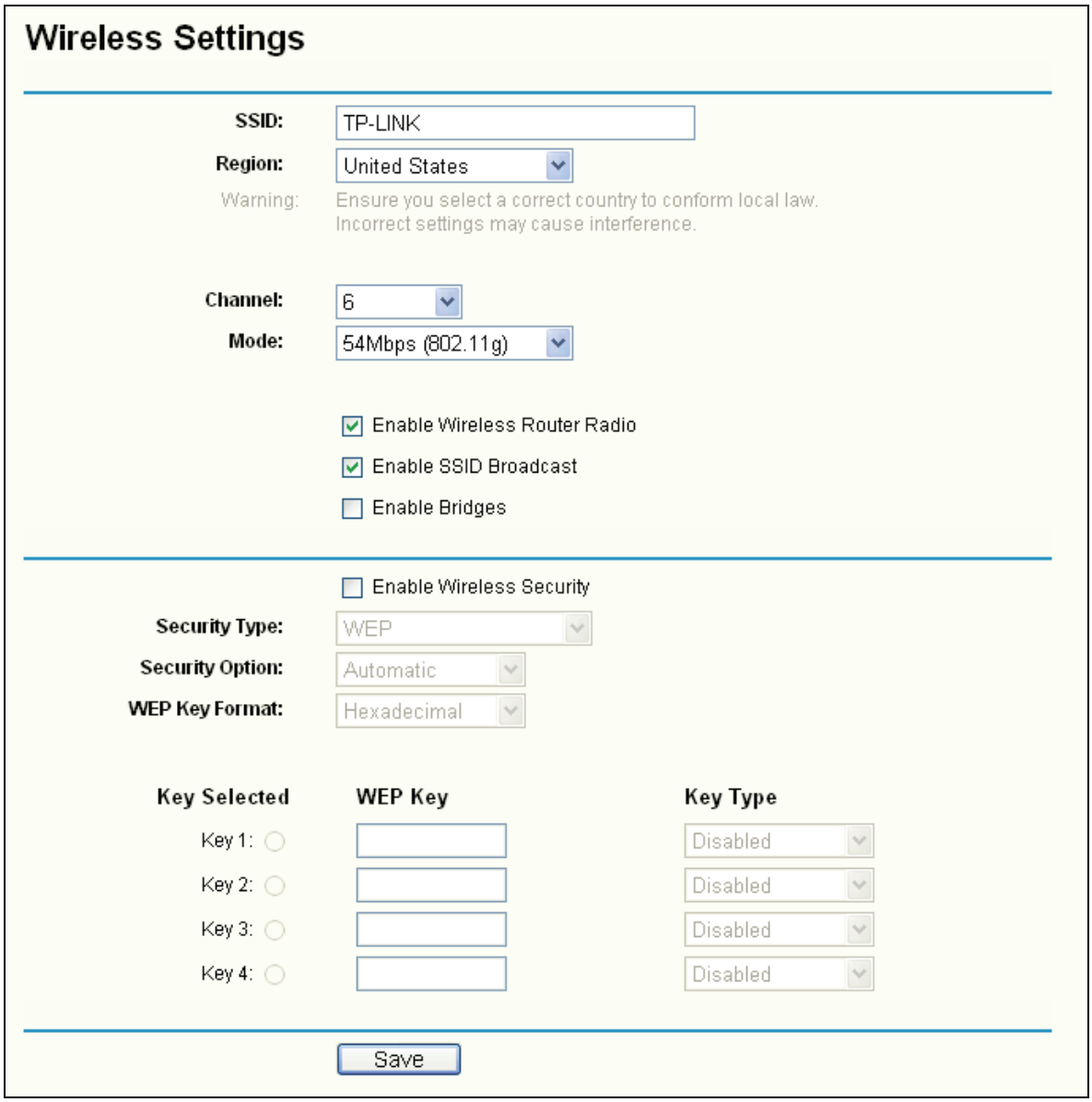
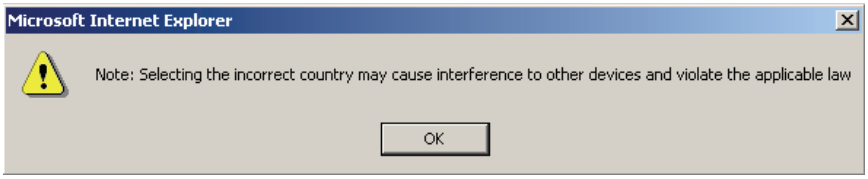


Figure 4-15 Wireless Settings

- **SSID -** Enter a value of up to 32 characters. The same name (SSID) must be assigned to all wireless devices in your network. The default SSID is TP-LINK, but it is recommended strongly that you change your networks name (SSID) to a different value. This value is case-sensitive. For example, *TP-LINK* is NOT the same as *tp-link*.
- **Region** - Select your region from the pull-down list. This field specifies the region where the wireless function of the router can be used. It may be illegal to use the wireless function of the router in a region other than one of those specified in this field. If your country or region is not listed, please contact your local government agency for assistance.

  The default region is United States. When you select your local region from the pull-down list, click the **Save** button, then the Note Dialog appears. Click OK.



Note Dialog

Note:

Limited by local law regulations, version for North America does not have region selection option.

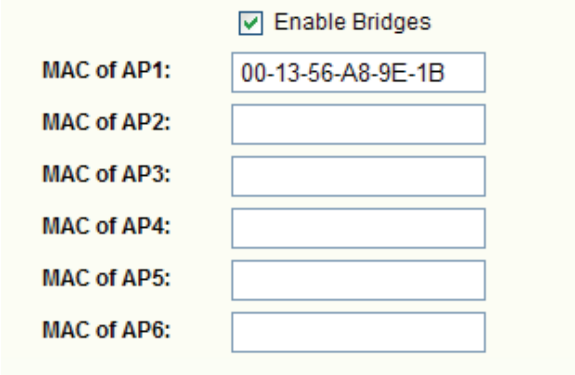
- **Channel -** This field determines which operating frequency will be used. It is not necessary to change the wireless channel unless you notice interference problems with another nearby access point.
- **Mode -** Select the desired wireless mode. The options are:
  - **54Mbps (802.11g) -** Both 802.11g and 802.11b wireless stations can connect to the router.
  - **11Mbps (802.11b) -** Only 802.11b wireless stations can connect to the router.

  Note:

  The default is "54Mbps (802.11g)", which allows both 802.11g and 802.11b wireless stations to connect to the router.
- **Enable Wireless Router Radio -** The wireless radio of this Router can be enabled or disabled to allow wireless stations access. If enabled, wireless stations will be able to access the router. Otherwise, wireless stations will not be able to access.
- **Enable SSID Broadcast -** If you select the **Enable SSID Broadcast** checkbox, the Wireless Router SSID will broadcast its name (SSID) on the air.
- **Enable Bridges** – If you select the **Enable Bridges** checkbox, you can input MAC address of other APs to communicate with them wirelessly in Bridge mode.
  - MAC of AP (1-6): Input the MAC address of the AP which you want to communicate with. There are six entries can be configured.

  The APs can communicate with each other in Bridge mode unless they know each other's MAC address. For example, if the router whose MAC address is 00-13-56-A8-9E-1A wants to communicate with an AP whose MAC address is 00-13-56-A8-9E-1B in Bridge mode, you should do as following:

  1. Select **Enable Bridges** and input 00-13-56-A8-9E-1B as following screen shown.



2. Access the AP's Web-based utility and configure the AP under Bridge mode, then input 00-13-56-A8-9E-1A in corresponding Blank.

- **Enable Wireless Security** – The wireless security function can be enabled or disabled. If disabled, the wireless stations will be able to connect the router without encryption. It is recommended strongly that you choose this option to encrypt your wireless network. The encryption settings are described below.
- **Authentication Type -** You can select one of the following authentication types:
  - **WEP -** Select WEP authentication type based on 802.11 authentications.
  - **WPA-PSK/WPA2-PSK -** Select WPA/WPA2 authentication type based on pre-shared pass phrase.
  - **WPA /WPA2 -** Select WPA/WPA2 authentication type based on Radius Server.
- **Authentication Options -** You can select one of the following authentication options:
  - When you select **WEP** for authentication type you can select the following authentication options:
  - **Automatic -** Select Shared Key or Open System authentication type automatically based on the wireless station request.
  - **Shared Key -** select 802.11 Shared Key authentications.
  - **Open System -** Select 802.11 Open System authentications.
  - When you select **WPA-PSK/WPA2-PSK** for authentication type you can select **Automatic**, **WPA –PSK** or **WPA2-PSK** as authentication options.
  - When you select **WPA/WPA2** as an authentication type you can select **Automatic WPA** or **WPA2** as authentication option.

- **WEP Key Format -** You can select **ASCII** or **Hexadecimal** format. ASCII Code Format stands for any combination of keyboard characters in the specified length. Hexadecimal format stands for any combination of hexadecimal digits (0-9, a-f, A-F) in the specified length.
- **WEP Key settings -** Select which of the four keys will be used and enter the matching WEP key information for your network in the selected key radio button. These values must be identical on all wireless stations in your network.
- **Key Type -** You can select the WEP key length (**64-bit**, or **128-bit,** or **152-bit**) for encryption. "Disabled" means the WEP key entry is invalid.
  - For **64-bit** encryption **-** You can enter 10 hexadecimal digits (any combination of 0-9, a-f, A-F, zero key is not permitted) or 5 ASCII characters.
  - For **128-bit** encryption **-** You can enter 26 hexadecimal digits (any combination of 0-9, a-f, A-F, zero key is not permitted) or 13 ASCII characters.
  - For **152-bit** encryption **-** You can enter 32 hexadecimal digits (any combination of 0-9, a-f, A-F, zero key is not permitted) or 16 ASCII characters.

- **Encryption -** When you select **WPA-PSK/WPA2-PSK** or **WPA/WPA2** for **Authentication Type** you can select **Automatic**, **TKIP** or **AES** as **Encryptions.**

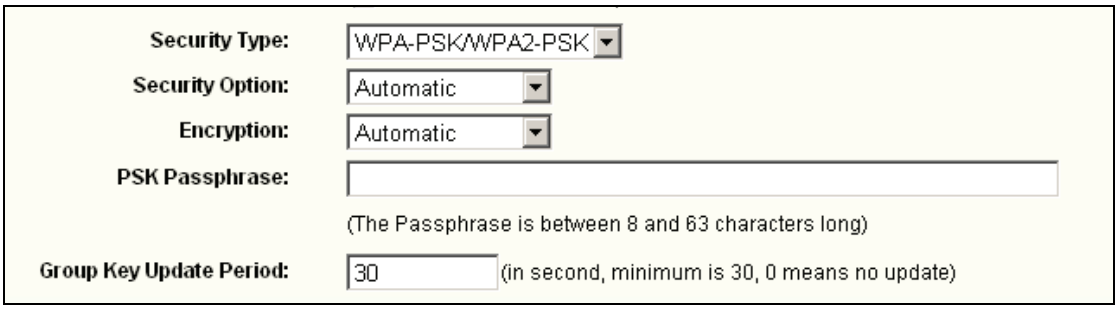


Figure 4-16 WPA-PSK/WPA2-PSK

- **WPA-PSK/WPA2-PSK Passphrase -** You can enter a WPA or WPA2 passphrase between 8 and 63 characters long.
- **Group Key Update Period -** Specify the group key update interval in seconds. The value can be either 0 seconds or from 30 seconds and up, 1-29 seconds are not usable figures. Enter 0 to disable the update.

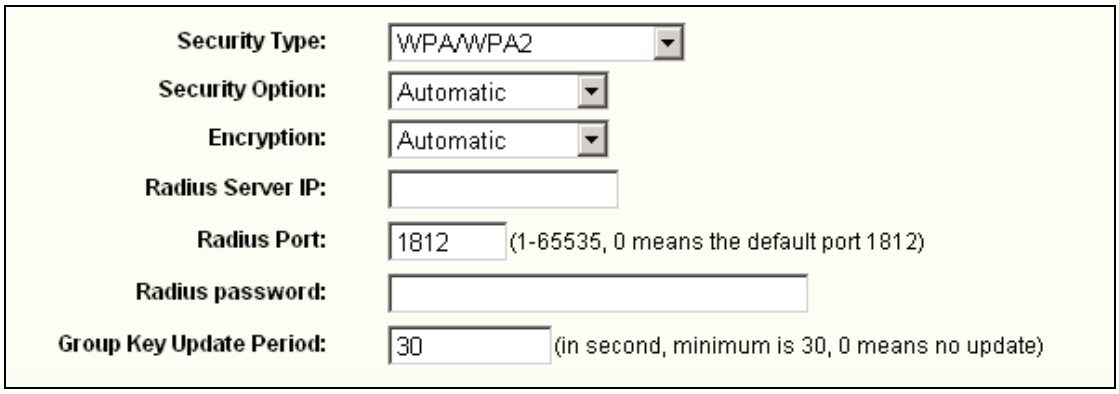


Figure 4-17 WPA/WPA2

- **Radius Server IP -** Enter the IP address of the Radius Server
- **Radius Port -** Enter the port number that the radius service used.
- **Radius Password -** Enter the password for the Radius Server.

Be sure to click the **Save** button to save your settings on this page.

Note: The router will reboot automatically after you click save.

4.5.2 MAC Filtering

The Wireless MAC Filtering for wireless networks is set on this page, Figure 4-18:

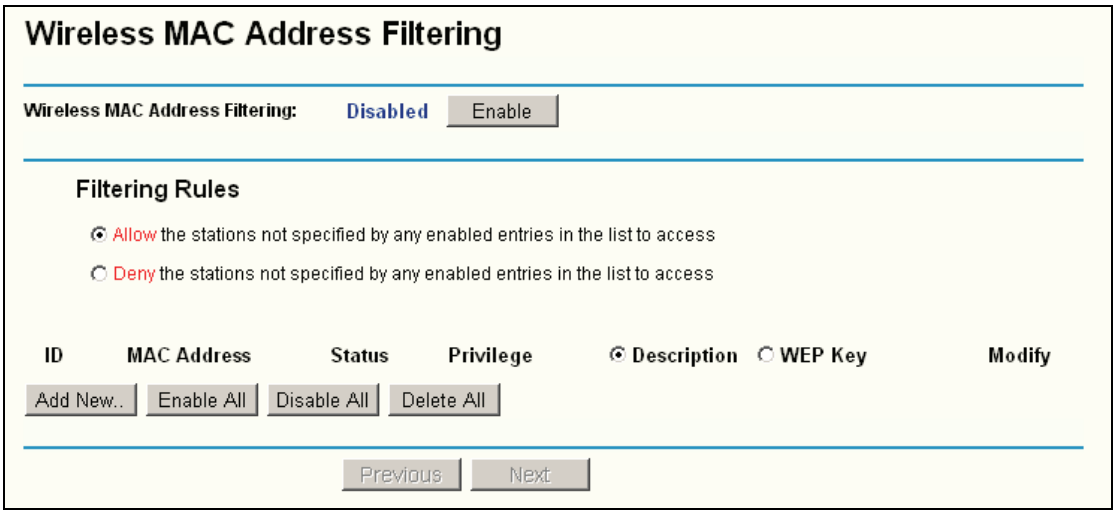


Figure 4-18 Wireless MAC address Filtering

The Wireless MAC Address Filtering feature allows you to control wireless stations accessing the router, which depend on the station's MAC addresses.

- **MAC Address -** The wireless station's MAC address that you want to access.
- **Status -** The status of this entry either **Enabled** or **Disabled**.
- **Privilege -** Select the privileges for this entry. You may select one of the following **Allow** /

Deny / **64-bit** / **128-bit** / **152-bit**.

- **Description -** A simple description of the wireless station.
- **WEP Key -** Specify a unique WEP key (in Hexadecimal format) to access the router.

To set up an entry, follow these instructions:

First, you must decide whether the unspecified wireless stations can access the router or not. If you desire that the unspecified wireless stations can access the router, please select the radio button **Allow the stations not specified by any enabled entries in the list to access**, otherwise, select the radio button **Deny the stations not specified by any enabled entries in the list to access**.

To Add a Wireless MAC Address filtering entry, click the **Add New…** button. The "**Add or Modify Wireless MAC Address Filtering entry"** page will appear, shown in Figure 4-19:

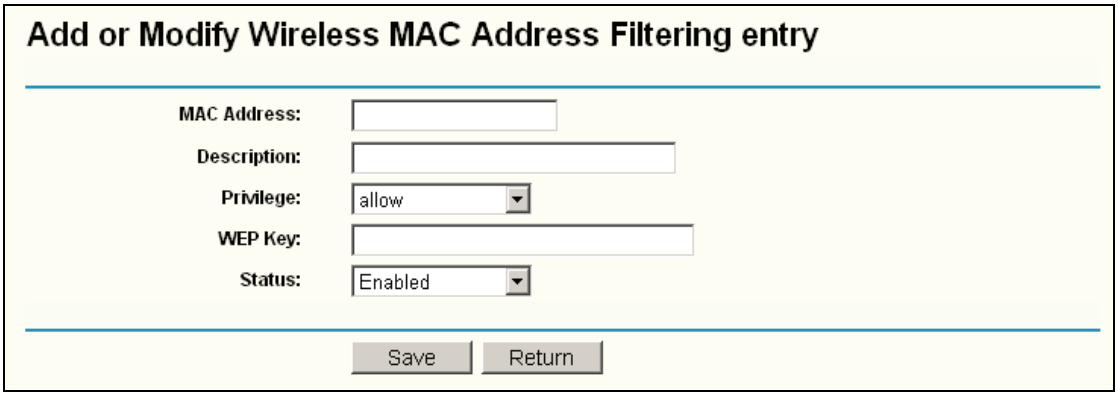


Figure 4-19 Add or Modify Wireless MAC Address Filtering entry

To add or modify a MAC Address Filtering entry, follow these instructions:

1. Enter the appropriate MAC Address into the **MAC Address** field. The format of the MAC Address is XX-XX-XX-XX-XX-XX (X is any hexadecimal digit). For example: 00-0A-EB-B0-00-0B.
2. Enter a simple description of the wireless station in the **Description** field. For example: Wireless station A.
3. **Privilege** - Select the privileges for this entry, one of **Allow** / **Deny** / **64-bit** / **128-bit** / **152-bit**.
4. WEP Key - If you select **64-bit**, **128-bit** or **152-bit** in the **Privilege** field, enter any combination of hexadecimal digits (0-9, a-f, A-F) in the specified length. For example: 2F34D20BE2.
5. **Status** - Select **Enabled** or **Disabled** for this entry on the **Status** pull-down list.
6. Click the **Save** button to save this entry.

To add additional entries, repeat steps 1-6.

☞ **Note:** When 64-bit, or 128-bit, or 152-bit is selected, WEP Key will be enabled.

To modify or delete an existing entry:

1. Click the **Modify** in the entry you want to modify. If you want to delete the entry, click the **Delete**.
2. Modify the information.
3. Click the **Save** button.

Click the **Enable All** button to make all entries enabled

Click the **Disabled All** button to make all entries disabled.

Click the **Delete All** button to delete all entries

Click the **Next** button to go to the next page and click the **Previous** button to return to the previous page.

For example: If you desire that the wireless station A with MAC address 00-0A-EB-00- 07-BE be able to access the router. The wireless station B with MAC address 00-0A-EB- 00-07-5F not be able to access the router, and the wireless station C with MAC address 00-0A-EB-00-07-8A be able to access the router when its WEP key is 2F34D20BE2E 54B326C5476586A, while all other wireless stations cannot access the router, you should configure the **Wireless MAC Address Filtering** list by following these steps:

1. Click the **Enable** button to enable this function.
2. Select the radio button: **Deny the stations not specified by any enabled entries in the list to access** for **Filtering Rules.**
3. Delete all or disable all entries if there are any entries already.
4. Click the **Add New...** button and enter the MAC address 00-0A-EB-00-07-BE in the **MAC Address** field, enter wireless station A in the **Description** field, select **Allow** in the **Privilege** pull-down list and select **Enabled** in the **Status** pull-down list. Click the **Save** and the **Return** button.
5. Click the **Add New...** button and enter the MAC address 00-0A-EB-00-07-5F in the **MAC Address** field, enter wireless station B in the **Description** field, select **Deny** in the **Privilege** pull-down list and select **Enabled** in the **Status** pull-down list. Click the **Save** and the **Return** button.
6. Click the **Add New...** button and enter the MAC address 00-0A-EB-00-07-8A in the **MAC Address** field, enter wireless station C in the **Description** field, select **128-bit** in the **Privilege** pull-down list, enter 2F34D20BE2E54B326C5476586A in the **WEP Key** field and select **Enabled** in the **Status** pull-down list. Click the **Save** and the **Return** button.

The filtering rules that configured should be similar to the following list:

ID	MAC Address	Status	Privilege	Description / WEP Key	Modify
1	00-0A-EB-00-07-BE	Enabled	allow	Wireless Station A	Modify Delete
2	00-0A-EB-00-07-5F	Enabled	deny	Wireless Station B	Modify Delete
3	00-0A-EB-00-07-8A	Enabled	128 bit	Wireless Station C	Modify Delete

☞ **Note:**

a) If you select the radio button **Allow the stations not specified by any enabled entries in the list to access** for **Filtering Rules,** the wireless station B will still not be able to access the router, however, other wireless stations that are not in the list will be able to access the router.

b) If you enable the function and select the **Deny the stations not specified by any enabled entries in the list to access** for **Filtering Rules,** and there are not any enable entries in the list, thus, no wireless stations can access the router.

4.5.3 Wireless Statistics

This page shows **MAC Address**, **Current Status**, **Received Packets** and **Sent Packets** for each connected wireless station.

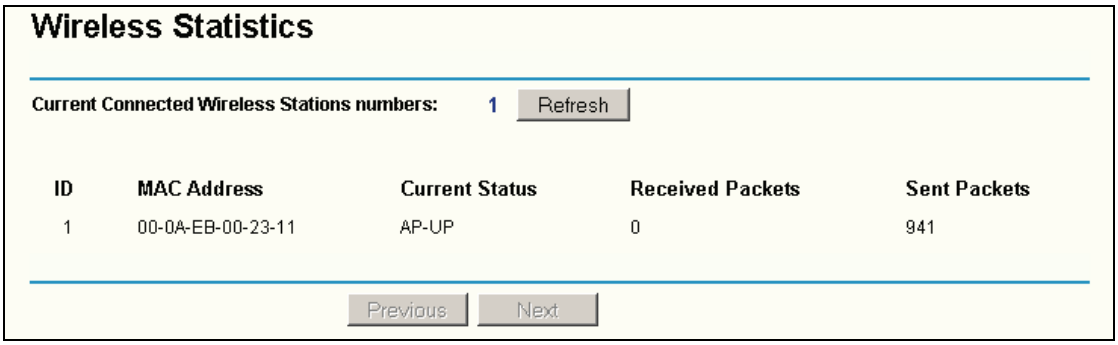


Figure 4-20 The router attached wireless stations

- **MAC Address -** The connected wireless station's MAC address
- **Current Status -** The connected wireless station's running status, one of STA-AUTH / STA-ASSOC / AP-UP / WPA / WPA-PSK /WPA2/WPA2-PSK/None
- **Received Packets -** Packets received by the station
- **Sent Packets -** Packets sent by the station

You cannot change any of the values on this page. To update this page and to show the current connected wireless stations, click on the **Refresh** button.

If the numbers of connected wireless stations go beyond one page, click the **Next** button to go to the next page and click the **Previous** button to return the previous page.

☞ **Note:** This page will be refreshed automatically every 5 seconds.

4.6 DHCP

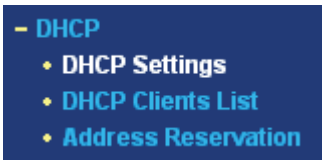


Figure 4-21 The DHCP menu

There are three submenus under the DHCP menu (shown in Figure 4-21): **DHCP Settings**, **DHCP Clients List** and **Address Reservation.** Click any of them, and you will be able to configure the corresponding function. The detailed explanations for each submenu are provided below.

4.6.1 DHCP Settings

The router is set up by default as a DHCP (Dynamic Host Configuration Protocol) server, which provides the TCP/IP configuration for all the PC(s) that are connected to the router on the LAN. The DHCP Server can be configured on the page (shown in Figure 4-22):

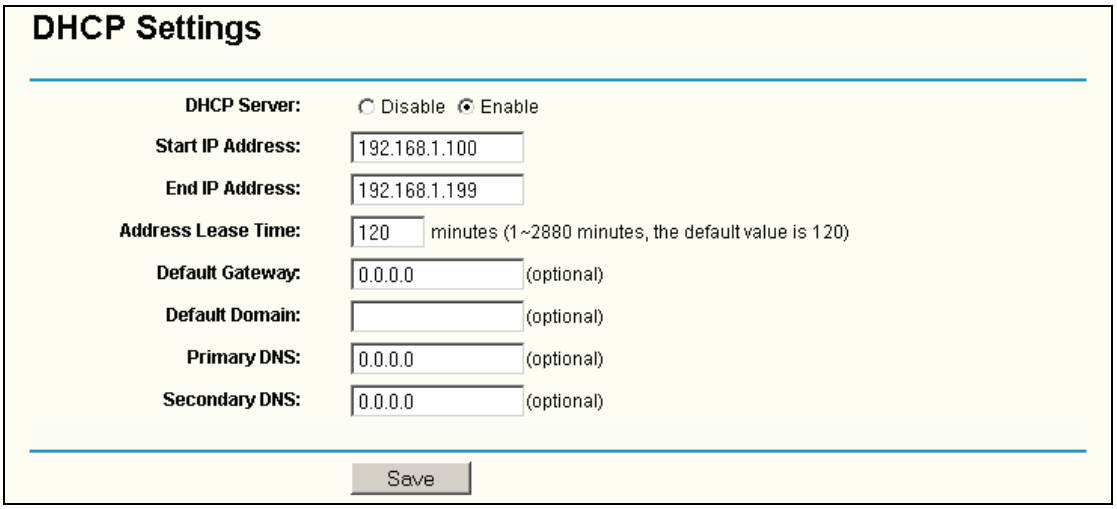


Figure 4-22 DHCP Settings

- **DHCP Server - Enable** or **Disable** the DHCP server. If you disable the Server, you must have another DHCP server within your network or else you must manually configure the computer.
- **Start IP Address -** This field specifies the first of the addresses in the IP address pool. 192.168.1.100 is the default start address.
- **End IP Address -** This field specifies the last of the addresses in the IP address pool. 192.168.1.199 is the default end address.
- **Address Lease Time -** The **Address Lease Time** is the amount of time in which a network user will be allowed connection to the router with their current dynamic IP Address. Enter the amount of time, in minutes. The user will be "leased" this dynamic IP Address. The range of

the time is 1 ~ 2880 minutes. The default value is 120 minutes.

- **Default Gateway -** (Optional.) Suggest to input the IP address of the LAN port of the router, default value is 192.168.1.1
- **Default Domain -** (Optional.) Input the domain name of your network.
- **Primary DNS -** (Optional.) Input the DNS IP address provided by your ISP. Or consult your ISP.
- **Secondary DNS -** (Optional.) Input the IP address of another DNS server if your ISP provides two DNS servers.

☞ **Note:**

To use the DHCP server function of the router, you must configure all computers on the LAN as "Obtain an IP Address automatically" mode. This function will take effect until the router reboots.

4.6.2 DHCP Clients List

This page shows **Client Name, MAC Address, Assigned IP,** and **Lease Time** for each DHCP Client attached to the router (Figure 4-23):

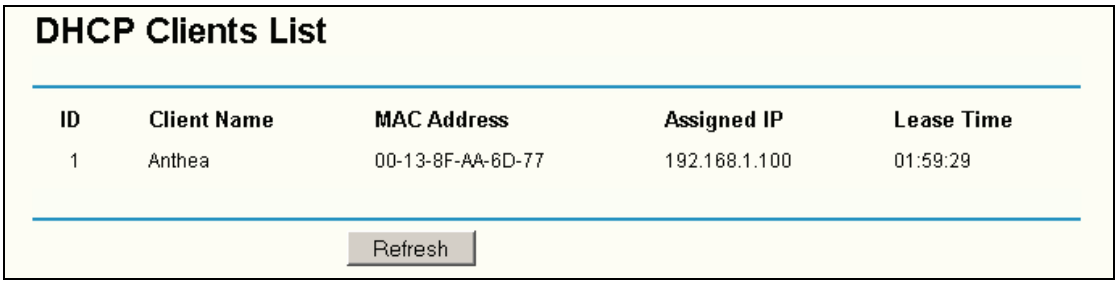


Figure 4-23 DHCP Clients List

- **Index -** The index of the DHCP Client
- **Client Name -** The name of the DHCP client
- **MAC Address -** The MAC address of the DHCP client
- **Assigned IP -** The IP address that the router has allocated to the DHCP client.
- **Lease Time -** The time of the DHCP client leased. Before the time is up, DHCP client will request to renew the lease automatically.

You cannot change any of the values on this page. To update this page and to show the current attached devices, click on the **Refresh** button.

4.6.3 Address Reservation

When you specify a reserved IP address for a PC on the LAN, that PC will always receive the same IP address each time when it accesses the DHCP server. Reserved IP addresses should

be assigned to servers that require permanent IP settings. This page is used for address reservation (shown in Figure 4-24).



Figure 4-24 Address Reservation

- **MAC Address -** The MAC address of the PC of which you want to reserve IP address.
- **Assigned IP Address -** The IP address of the router reserved.
- **Status -** The status of this entry either **Enabled** or **Disabled**.

To Reserve IP addresses:

1. Click the **Add New button**. (Pop-up Figure 4-25)
2. Enter the MAC address (The format for the MAC Address is XX-XX-XX-XX-XX-XX.) and IP address in dotted-decimal notation of the computer you wish to add.
3. Click the **Save** button when finished.

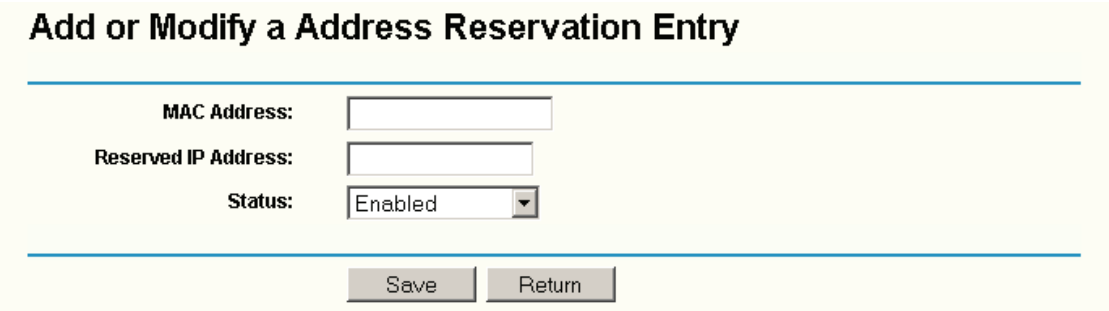


Figure 4-25 Add or Modify an Address Reservation Entry

To modify or delete an existing entry:

1. Click the **Modify** in the entry you want to modify. If you want to delete the entry, click the **Delete**.
2. Modify the information.
3. Click the **Save** button.

Click the **Enable All** button to make all entries enabled

Click the **Disabled All** button to make all entries disabled.

Click the **Delete All** button to delete all entries

Click the **Next** button to go to the next page and Click the **Previous** button to return the previous page.

☞ **Note:** The function won't take effect until the router reboots.

4.7 Forwarding



Figure 4-26 The Forwarding menu

There are four submenus under the Forwarding menu (shown in Figure 4-26): **Virtual Servers**, **Port Triggering**, **DMZ** and **UPnP**. Click any of them, and you will be able to configure the corresponding function. The detailed explanations for each submenu are provided below.

4.7.1 Virtual Servers

Virtual servers can be used for setting up public services on your LAN, such as DNS, Email and FTP. A virtual server is defined as a service port, and all requests from the Internet to this service port will be redirected to the computer specified by the server IP. Any PC that was used for a virtual server must have a static or reserved IP Address because its IP Address may change when using the DHCP function. You can set up virtual servers on this page, shown in Figure 4-27:

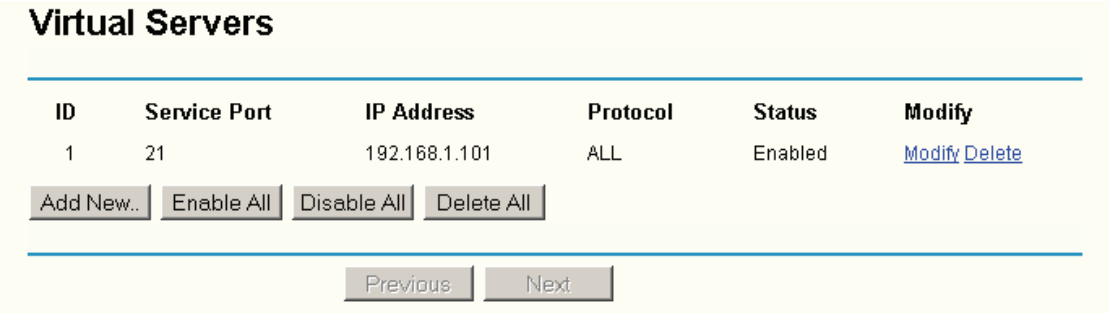


Figure 4-27 Virtual Servers

- **Service Port -** The numbers of External Ports. You can type a service port or a range of service ports (the format is XXX – YYY, XXX is the start port, YYY is the end port).
- **IP Address -** The IP Address of the PC providing the service application.
- **Protocol -** The protocol used for this application, either **TCP**, **UDP**, or **All** (all protocols supported by the router).
- **Status -** The status of this entry either **Enabled** or **Disabled**.

To setup a virtual server entry:

1. Click the **Add New button**. (pop-up Figure 4-28)
2. Select the service you want to use from the Common Service Port list. If the **Common Service Port** list does not have the service that you want to use, type the number of the service port or service port range in the **Service Port** box.
3. Type the IP Address of the computer in the **Server IP Address** box.
4. Select the protocol used for this application, either **TCP** or **UDP**, or **All**.
5. Select the **Enable** checkbox to enable the virtual server.
6. Click the **Save** button.

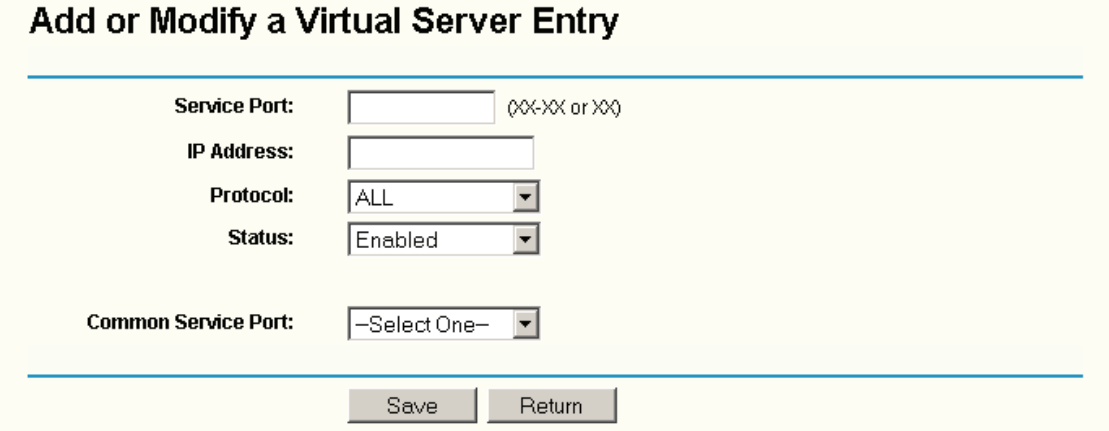


Figure 4-28 Add or Modify a Virtual Server Entry

☞ **Note:**

It is possible that you have a computer or server that has more than one type of available service. If so, select another service, and enter the same IP Address for that computer or server.

To modify or delete an existing entry:

1. Click the **Modify** in the entry you want to modify. If you want to delete the entry, click the **Delete**.
2. Modify the information.
3. Click the **Save** button.

Click the **Enable All** button to make all entries enabled

Click the **Disabled All** button to make all entries disabled.

Click the **Delete All** button to delete all entries

Click the **Next** button to go to the next page and Click the **Previous** button to return the previous page.

☞ **Note:**

If you set the virtual server of service port as 80, you must set the Web management port on **Security –> Remote Management** page to be any value except 80 such as 8080. Or else there will be a conflict to disable the virtual server.

4.7.2 Port Triggering

Some applications require multiple connections, like Internet games, video conferencing, Internet calling and so on. These applications cannot work with a pure NAT router. Port Triggering is used for some of these applications that can work with an NAT router. You can set up Port Triggering on this page shown in Figure 4-29:

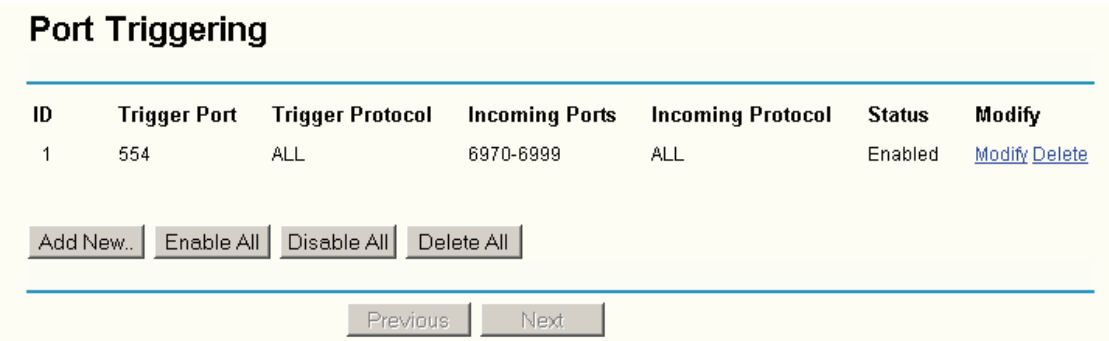


Figure 4-29 Port Triggering

Once configured, operation is as follows:

1. A local host makes an outgoing connection using a destination port number defined in the Trigger Port field.
2. The router records this connection, opens the incoming port or ports associated with this entry in the Port Triggering table, and associates them with the local host.
3. When necessary the external host will be able to connect to the local host using one of the ports defined in the **Incoming Ports** field.

- **Trigger Port -** The port for outgoing traffic. An outgoing connection using this port will "Trigger" this rule.
- **Trigger Protocol -** The protocol used for Trigger Ports, either **TCP**, **UDP**, or **All** (all protocols supported by the router).
- **Incoming Ports Range -** The port or port range used by the remote system when it responds to the outgoing request. A response using one of these ports will be forwarded to the PC that triggered this rule. You can input at most 5 groups of ports (or port section). Every group of ports must be set apart with ",". For example, 2000-2038, 2050-2051, 2085, 3010-3030.
- **Incoming Protocol -** The protocol used for Incoming Ports Range, either TCP or UDP, or ALL (all protocols supported by the router).

- **Status -** The status of this entry either **Enabled** or **Disabled**.

To add a new rule, enter the following data on the **Port Triggering** screen.

1. Click the **Add New button**. (pop-up Figure 4-30)
2. Enter a port number used by the application when it generates an outgoing request.
3. Select the protocol used for **Trigger Port** from the pull-down list, either **TCP**, **UDP**, or **All.**
4. Enter the range of port numbers used by the remote system when it responds to the PC's request.
5. Select the protocol used for **Incoming Ports Range** from the pull-down list, either **TCP** or **UDP**, or **All.**
6. Select the **Enable** checkbox to enable.
7. Click the **Save** button to save the new rule.

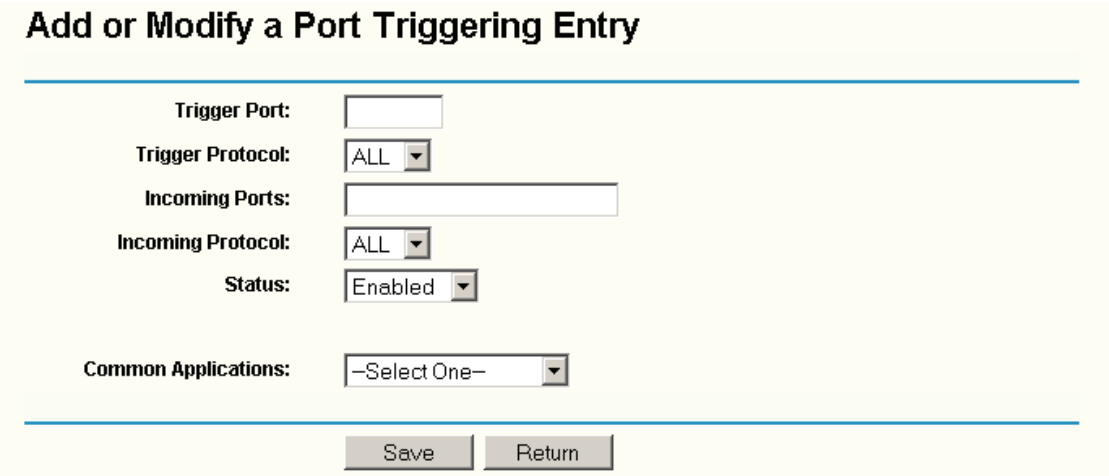


Figure 4-30 Add or Modify a Triggering Entry

There are many popular applications in the **Popular Application** list. You can select it, and the application will fill in the **Trigger Port**, **incoming Ports Range** boxes and select the **Enable** checkbox. It has the same effect as adding a new rule.

To modify or delete an existing entry:

1. Click the **Modify** in the entry you want to modify. If you want to delete the entry, click the **Delete**.
2. Modify the information.
3. Click the **Save** button.

Click the **Enable All** button to make all entries enabled

Click the **Disabled All** button to make all entries disabled.

Click the **Delete All** button to delete all entries

☞ **Note:**

1. When the trigger connection is released, the according opening ports will be closed.
2. Each rule allowed to be used only by one host on LAN synchronously. The trigger connection of other hosts on LAN will be refused.
3. Incoming Port Range cannot overlap each other.

4.7.3 DMZ

The DMZ host feature allows one local host to be exposed to the Internet for a special-purpose service such as Internet gaming or videoconferencing. DMZ host forwards all the ports at the same time. Any PC whose port is being forwarded must have its DHCP client function disabled and should have a new static IP Address assigned to it because its IP Address may change when using the DHCP function. You can set up DMZ host on this page shown in Figure 4-31:

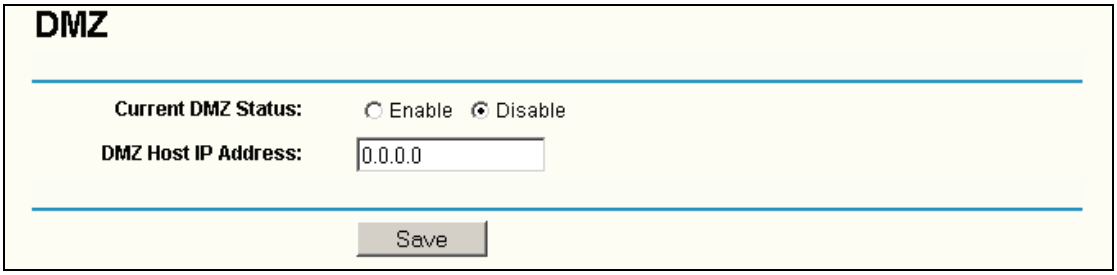


Figure 4-31 DMZ

To assign a computer or server to be a DMZ server:

1. Click the **Enable** radio button
2. Enter the local host IP Address in the **DMZ Host IP Address** field
3. Click the **Save** button.

☞ **Note:**

After you set the DMZ host, the firewall related to the host will not work.

4.7.4 UPnP

The Universal Plug and Play (UPnP) feature allows the devices, such as Internet computers, to access the local host resources or devices as needed. UPnP devices can be automatically discovered by the UPnP service application on the LAN. You can configure UPnP on this page that shown in Figure 4-32:

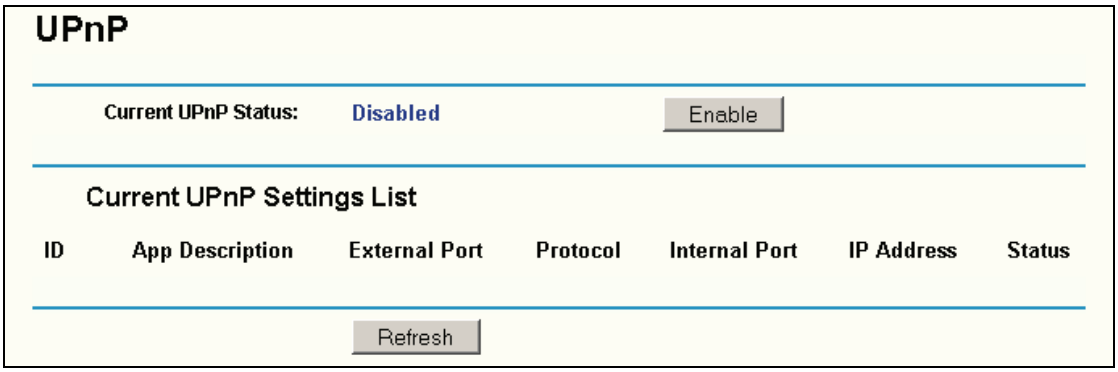


Figure 4-32 UPnP Setting

- **Current UPnP Status -** UPnP can be enabled or disabled by clicking the **Enable** or **Disable** button. As allowing this may present a risk to security, this feature is disabled by default.
- **Current UPnP Settings List -** This table displays the current UPnP information.
  - **App Description** – The description provided by the application in the UPnP request
  - **External Port -** External port, which the router opened for the application.
  - **Protocol –** Shows which type of protocol is opened.
  - **Internal Port -** Internal port, which the router opened for local host.
  - **IP Address -** The UPnP device that is currently accessing the router.
  - **Status -** Either Enabled or Disabled, "Enabled" means that port is still active. Otherwise, the port is inactive.

Click **Refresh** to update the Current UPnP Settings List.

4.8 Security



Figure 4-33 The Security menu

There are six submenus under the Security menu (shown in Figure 4-33): **Firewall**, **IP Address Filtering, Domain Filtering, MAC Filtering, Remote Management** and **Advanced Security.** Click any of them, and you will be able to configure the corresponding function. The detailed explanations for each submenu are provided below.

4.8.1 Firewall

Using the Firewall page (shown in Figure 4-34), you can turn the general firewall switch on or off. The default setting for the switch is off. If the general firewall switch is off, even if IP Address Filtering, DNS Filtering and MAC Filtering are enabled, their settings are ineffective.

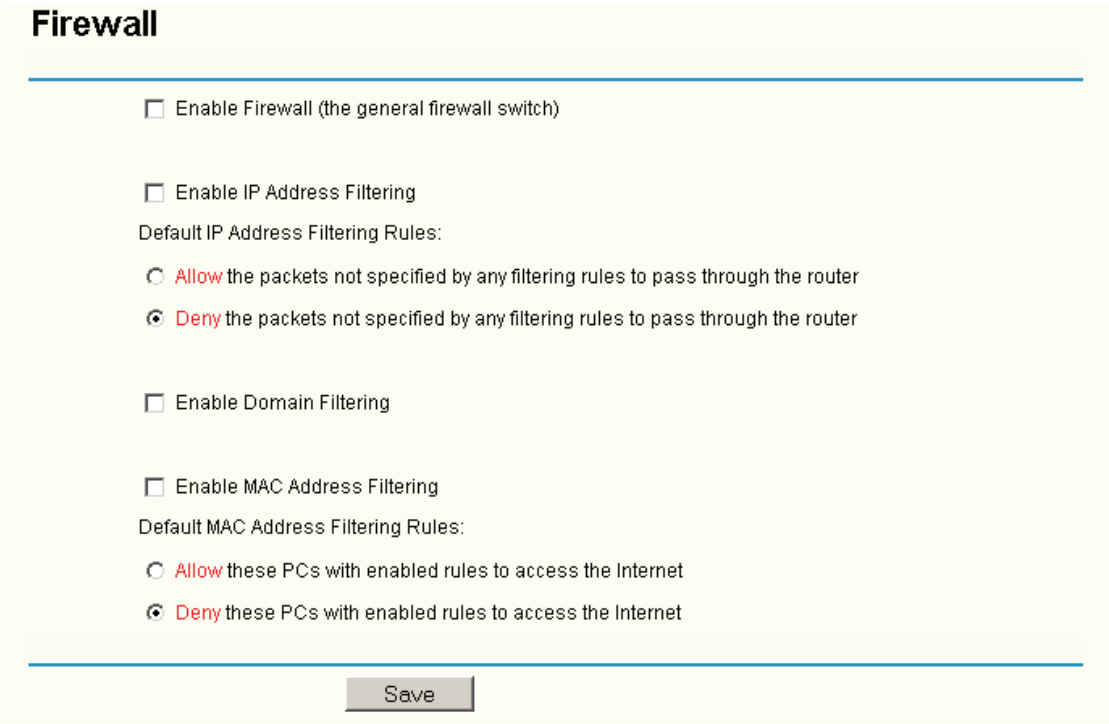


Figure 4-34 Firewall Settings

- **Enable Firewall -** the general firewall switch is on or off.
- **Enable IP Address Filtering -** set IP Address Filtering is enabled or disabled. There are two default filtering rules of IP Address Filtering, either Allow or Deny passing through the router.
- **Enable Domain Filtering -** set Domain Filtering is enabled or disabled.
- **Enable MAC Filtering -** set MAC Address Filtering is enabled or disabled. You can select the default filtering rules of MAC Address Filtering, either Allow or Deny accessing the router.

4.8.2 IP Address Filtering

The IP address Filtering feature allows you to control Internet Access by specific users on your LAN based on their IP addresses. The IP address filtering is set on this page, Figure 4-35:

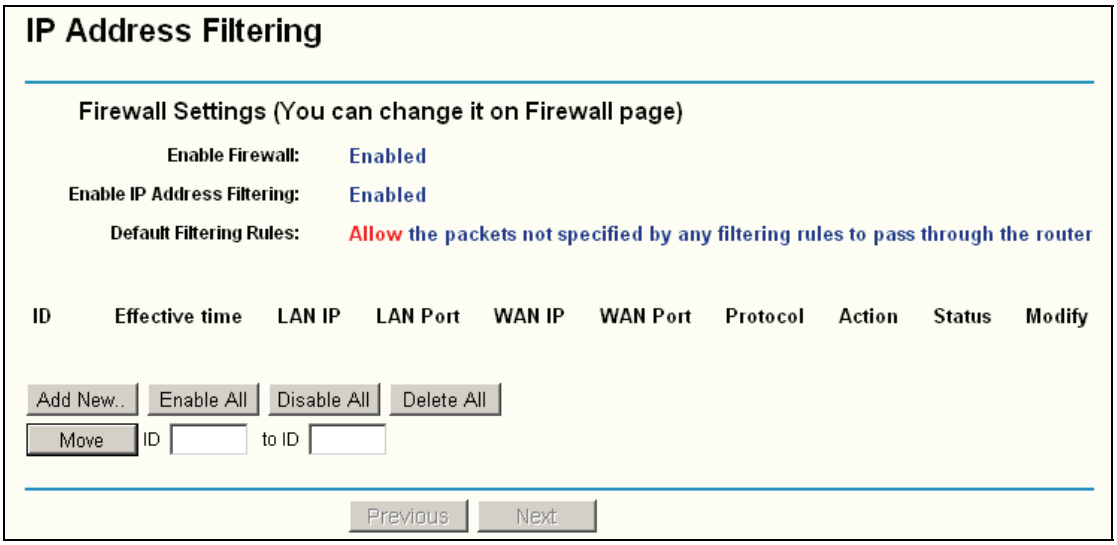


Figure 4-35 IP address Filtering

To disable the IP Address Filtering feature, keep the default setting, **Disabled**. To set up an IP Address Filtering entry, click **Enable** Firewall and **Enable** IP Address Filtering on the Firewall page, and click the **Add New…** button. The page "**Add or Modify an IP Address Filtering entry**" will appear shown in Figure 4-36:

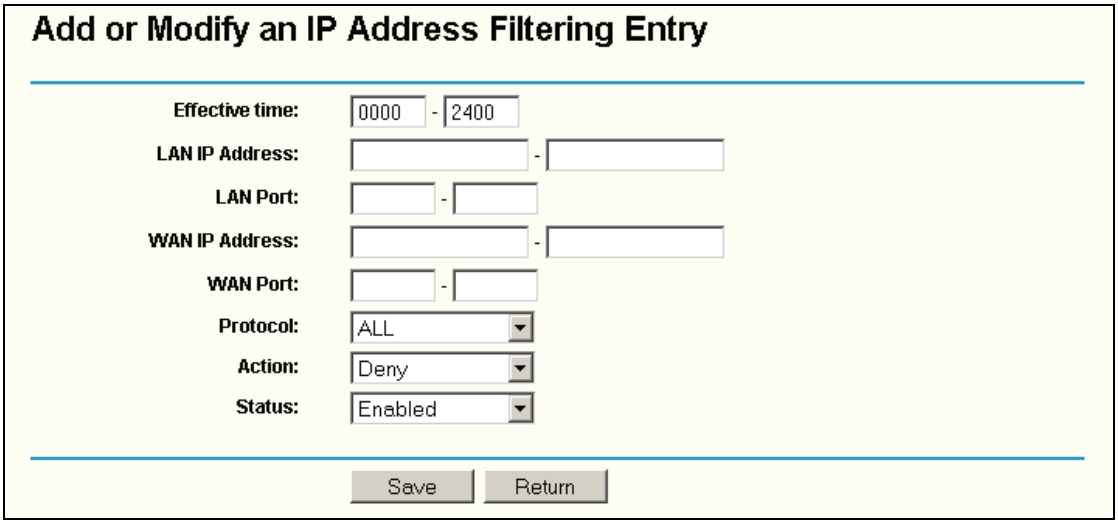


Figure 4-36 Add or Modify an IP Address Filtering Entry

To create or modify an IP Address Filtering entry, please follow these instructions:

1. **Effective Time -** Enter a range of time in HHMM format, which point to the range time for the entry to take effect. For example, 0803 - 1705, the entry will take effect from 08:03 to 17:05.

2. **LAN IP Address -** Enter a LAN IP Address or a range of LAN IP addresses in the field, in dotted-decimal notation format. For example, 192.168.1.20 - 192.168.1.30. Keep the field open, which means all LAN IP Addresses have been put into the field.

3. **LAN Port -** Enter a LAN Port or a range of LAN ports in the field. For example, 1030 - 2000. Keep the field open, which means all LAN ports have been put into the field.

4. **WAN IP Address -** Enter a WAN IP Address or a range of WAN IP Addresses in the field, in dotted-decimal notation format. For example, 61.145.238.6 – 61.145.238.47. Keep the field open, which means all WAN IP Addresses have been put into the field.
5. **WAN Port -** Enter a WAN Port or a range of WAN Ports in the field. For example, 25 – 110. Keep the field open, which means all WAN Ports have been put into the field.
6. **Protocol -** Select which protocol is to be used, either **TCP, UDP**, or **All** (all protocols supported by the router).
7. **Action -** Select either **Allow** or **Deny** through the router.
8. **Status -** Select **Enabled** or **Disabled** for this entry on the **Status** pull-down list.
9. Click the **Save** button to save this entry.

To modify or delete an existing entry:

1. Click the **Modify** in the entry you want to modify. If you want to delete the entry, click the **Delete**.
2. Modify the information.
3. Click the **Save** button.

Click the **Enable All** button to make all entries enabled

Click the **Disabled All** button to make all entries disabled.

Click the **Delete All** button to delete all entries

You can change the entry's order as desired. Fore entries are before hind entries. Enter the ID number in the first box you want to move and another ID number in second box you want to move to, and then click the **Move** button to change the entry's order.

Click the **Next** button to the next page and click the **Previous** button to return to the previous page.

For example: If you desire to block E-mail received and sent by the IP Address 192.168.1.7 on your local network, and to make the PC with IP Address 192.168.1.8 unable to visit the website of IP Address 202.96.134.12, while other PC(s) have no limit you should specify the following IP address filtering list:

ID	Effective time	LAN IP	LAN Port	WAN IP	WAN Port	Protocol	Action	Status	Modify
1	0000-2400	192.168.1.7	-	-	25	ALL	Deny	Enabled	Modify Delete
2	0000-2400	192.168.1.7	-	-	110	ALL	Deny	Enabled	Modify Delete
3	0000-2400	192.168.1.8	-	202.96.134.12	-	ALL	Deny	Enabled	Modify Delete

4.8.3 Domain Filtering

The Domain Filtering page (shown in Figure 4-37) allows you to control access to certain websites on the Internet by specifying their domains or key words.

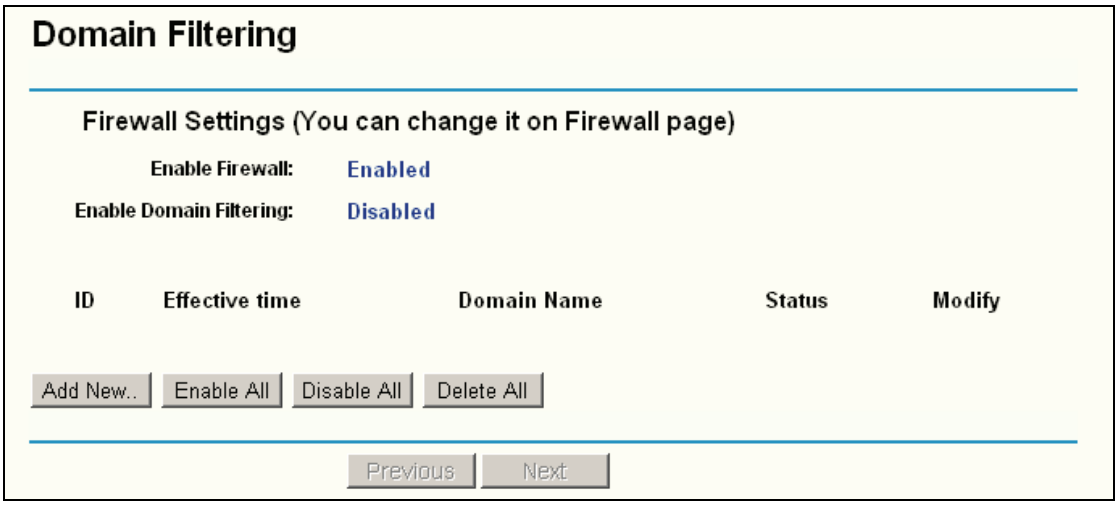


Figure 4-37 Domain Filtering

Before adding a Domain Filtering entry, you must ensure that **Enable** Firewall and **Enable** Domain Filtering have been selected on the Firewall page. To Add a Domain filtering entry, click the **Add New…** button. The page "**Add or Modify a Domain Filtering entry**" will appear, shown in Figure 4-38:

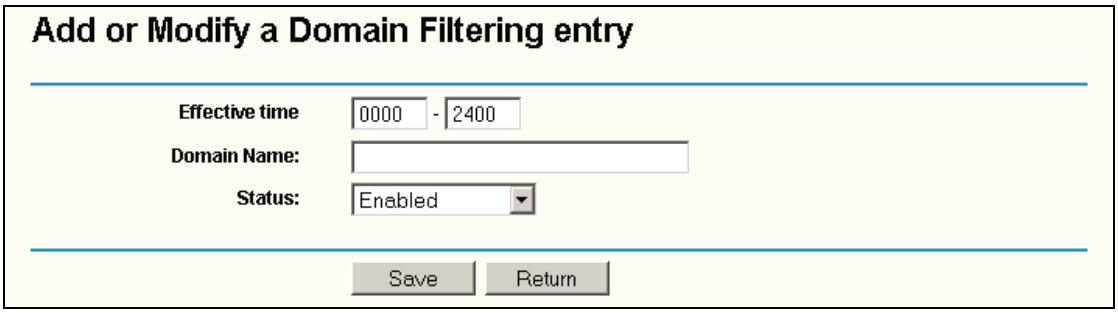


Figure 4-38 Add or Modify a Domain Filtering entry

To add or modify a Domain Filtering entry, follow these instructions:

1. **Effective Time -** Enter a range of time in HHMM format specifying the time for the entry to take effect. For example, if you enter: 0803 - 1705, than the entry will take effect from 08:03 to 17:05.

2. **Domain Name -** Type the domain or key word as desired in the field. A blank in the domain field means all websites on the Internet. For example: www.xxyy.com.cn, .net.

3. **Status -** Select **Enabled** or **Disabled** for this entry on the **Status** pull-down list.
4. Click the **Save** button to save this entry.

To modify or delete an existing entry:

1. Click the **Modify** in the entry you want to modify. If you want to delete the entry, click the **Delete**.
2. Modify the information.
3. Click the **Save** button.

Click the **Enabled All** button to make all entries enabled.

Click the **Disabled All** button to make all entries disabled.

Click the **Delete All** button to delete all entries

Click the **Next** button to go to the next page and the **Previous** button to return to the previous page.

For example, if you want to block the PC(s) on your LAN to access websites www.xxyy.com.cn, www.aabbcc.com and websites with .net in the end on the Internet while no limit for other websites, you should specify the following Domain filtering list:

ID	Effective time	Domain Name	Status	Modify
1	0000-2400	www.xxyy.com	Enabled	Modify Delete
2	0800-2000	www.aabbcc.com	Enabled	Modify Delete
3	0000-2400	.net	Enabled	Modify Delete

4.8.4 MAC Filtering

Like the IP Address Filtering page, the MAC Address Filtering page (shown in Figure 4-39) allows you to control access to the Internet by users on your local network based on their MAC Address.

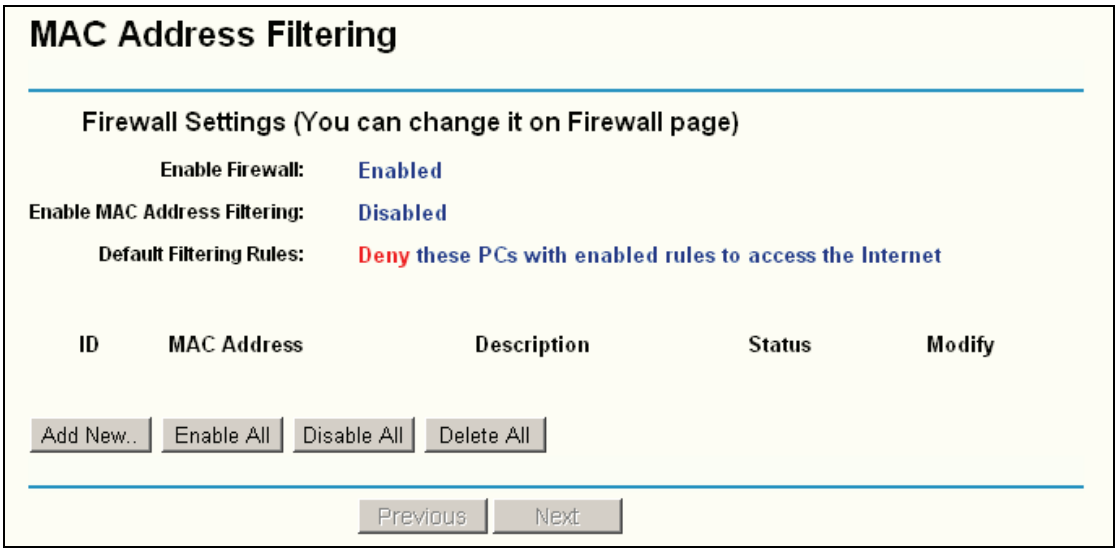


Figure 4-39 MAC address Filtering

Before setting up MAC Filtering entries, you must ensure that **Enable** Firewall and **Enable** MAC Filtering have been selected on the Firewall page. To Add a MAC Address filtering entry, clicking the **Add New…** button. The page "**Add or Modify a MAC Address Filtering entry**" will appear, shown in Figure 4-40:

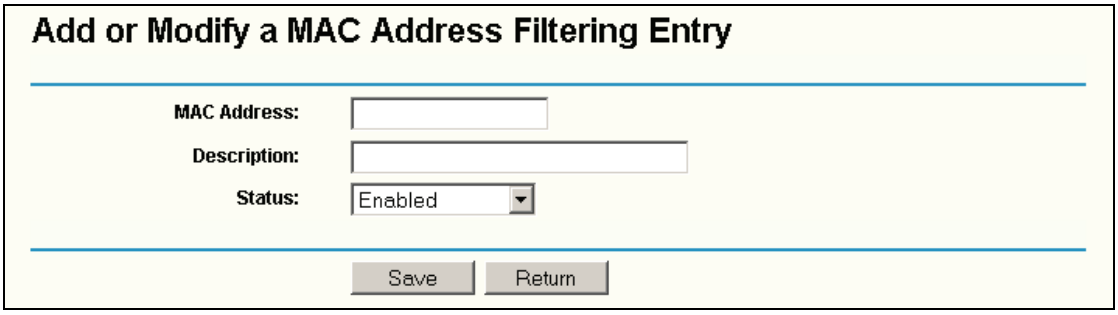


Figure 4-40 Add or Modify a MAC Address Filtering entry

To add or modify a MAC Address Filtering entry, follow these instructions:

1. Enter the appropriate MAC Address into the **MAC Address** field. The format of the MAC Address is XX-XX-XX-XX-XX-XX (X is any hexadecimal digit). For example: 00-0E-AE-B0-00-0B.
2. Type the description of the PC in the **Description** field. Fox example: John's PC.
3. **Status** - Select **Enabled** or **Disabled** for this entry on the **Status** pull-down list.
4. Click the **Save** button to save this entry.

To add additional entries, repeat steps 1-4.

When finished, click the **Return** button to return to the **MAC Address Filtering** page.

To modify or delete an existing entry:

1. Click the **Modify** in the entry you want to modify. If you want to delete the entry, click the **Delete**.
2. Modify the information.
3. Click the **Save** button.

Click the **Enable All** button to make all entries enabled.

Click the **Disabled All** button to make all entries disabled.

Click the **Delete All** button to delete all entries

Click the **Next** button to go to the next page and click the **Previous** button to return to the previous page.

Fox example: If you want to block the PC with MAC addresses 00-0A-EB-00-07-BE and 00-0A-EB-00-07-5F to access the Internet, first, enable the **Firewall** and **MAC Address Filtering** on the **Firewall** page, then, you should specify the Default MAC Address Filtering Rule "**Deny these PC(s) with effective rules to access the Internet**" on the Firewall page and the following MAC address filtering list on this page:

ID	MAC Address	Description	Status	Modify
1	00-0A-EB-00-07-BE	John's computer	Enabled	Modify Delete
2	00-0A-EB-00-07-5F	Alice's computer	Enabled	Modify Delete

4.8.5 Remote Management

You can configure the Remote Management function on this page shown in Figure 4-41. This feature allows you to manage your Router from a remote location, via the Internet.

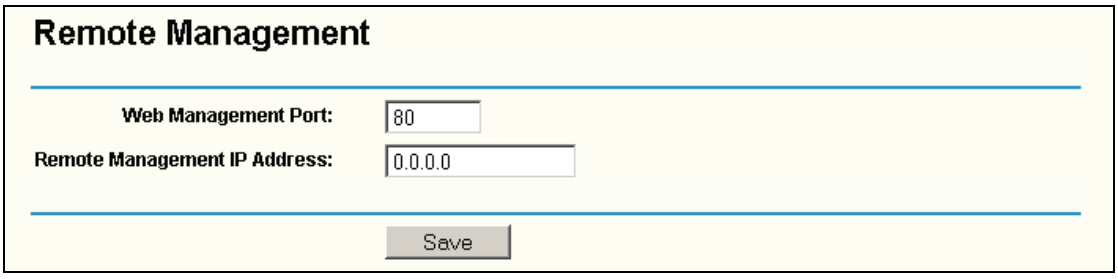


Figure 4-41 Remote Management

- **Web Management Port -** Web browser access normally uses the standard HTTP service port 80. This router's default remote management Web port number is 80. For greater security, you can change the remote management Web interface to a custom port by entering that number in this box provided. Choose a number between 1024 and 65534, but do not use the number of any common service port.

- **Remote Management IP Address -** This is the current address you will use when accessing your router from the Internet. The default IP Address is 0.0.0.0. It means this function is disabled. To enable this function, change the default IP Address to another IP Address as desired.

To access the router, you will type your router's WAN IP Address into your browser's Address (in IE) or Location (in Navigator) box, followed by a colon and the custom port number. For example, if your Router's WAN address is 202.96.12.8 and you use port number 8080, enter in your browser: http://202.96.12.8:8080. You will be asked for the router's password. After successfully entering the password, you will be able to access the router's Web-based utility.

☞ **Note:** Be sure to change the router's default password to a very secure password.

4.8.6 Advanced Security

Using Advanced Security page (shown in Figure 4-42), you can protect the router from being attacked by TCP-SYN Flood, UDP Flood and ICMP-Flood from LAN.

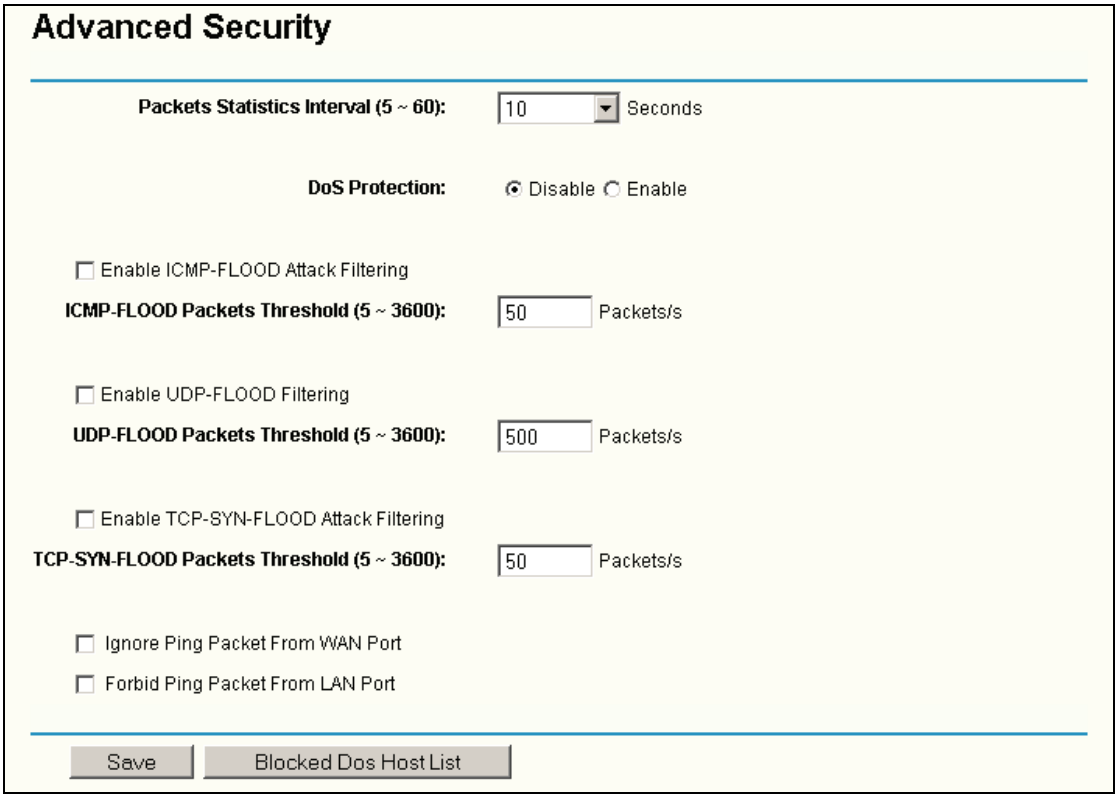


Figure 4-42 Advanced Security settings

- **Packets Statistic interval (5 ~ 60) -** The default value is 10. Select a value between 5 and 60 seconds in the pull-down list. The **Packets Statistic interval** value indicates the time section of the packets statistic. The result of the statistic used for analysis by **SYN Flood**, **UDP Flood** and **ICMP-Flood**.
- **DoS protection - Enable** or **Disable** the DoS protection function. Only when it is enabled, will the flood filters be effective.

- **Enable ICMP-FLOOD Attack Filtering - Enable** or **Disable** the **ICMP-FLOOD** Attack Filtering.
- **ICMP-FLOOD Packets threshold: (5 ~ 3600) -** The default value is 50. Enter a value between 5 ~ 3600 packets. When the current **ICMP-FLOOD** Packets numbers is beyond the set value, the router will start up the blocking function immediately.
- **Enable UDP-FLOOD Filtering - Enable** or **Disable** the **UDP-FLOOD** Filtering.
- **UDP-FLOOD Packets threshold: (5 ~ 3600) -** The default value is 50. Enter a value between 5 ~ 3600 packets. When the current **UPD-FLOOD** Packets numbers is beyond the set value, the router will start up the blocking function immediately.
- **Enable TCP-SYN-FLOOD Attack Filtering - Enable** or **Disable** the **TCP-SYN- FLOOD** Attack Filtering.
- **TCP-SYN-FLOOD Packets threshold: (5 ~ 3600) -** The default value is 50. Enter a value between 5 ~ 3600 packets. When the current **TCP-SYN-FLOOD** Packets numbers is beyond the set value, the router will start up the blocking function immediately.
- **Ignore Ping Packet from WAN Port - Enable** or **Disable** ignore ping packet from WAN port. The default is disabled. If enabled, the ping packet from the Internet cannot access the router.
- **Forbid Ping Packet from LAN Port -** Enable or Disable forbidding Ping Packet to access the router from the LAN port. The default value is disabled. If enabled, the ping packet from the LAN port cannot access the router. (Defends against some viruses)

Click the **Save** button to save the settings.

Click the **Blocked DoS Host Table** button to display the DoS host table by blocking. The page will appear that shown in Figure 4-43:

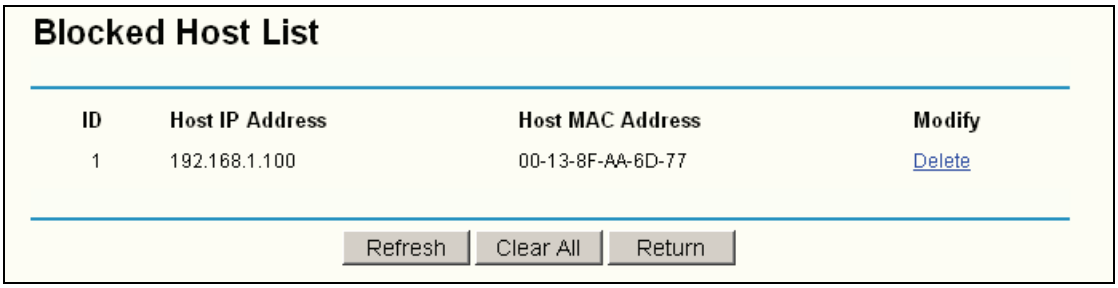


Figure 4-43 Thwarted DoS Host Table

This page shows **Host IP Address** and **Host MAC Address** for each host blocked by the router.

- **Host IP Address-** The IP address that blocked by DoS are displayed here.
- **Host MAC Address -** The MAC address that blocked by DoS are displayed here.

To update this page and to show the current blocked host, click on the **Refresh** button.

Click the **Clear All** button to clear all displayed entries. After the table is empty the blocked host

will regain the capability to access Internet.

Click the **Return** button to return to the **Advanced Security** page.

4.9 IP & MAC Binding Setting



Figure 4-44 the IP & MAC Binding menu

There are two submenus under the IP &MAC Binding menu (shown in Figure 4-44): **Binding Setting** and **ARP List**. Click any of them, and you will be able to scan or configure the corresponding function. The detailed explanations for each submenu are provided below.

4.9.1 Binding Setting

This page displays the IP & MAC Binding Setting table; you can operate it in accord with your desire. (shown in Figure 4-45).

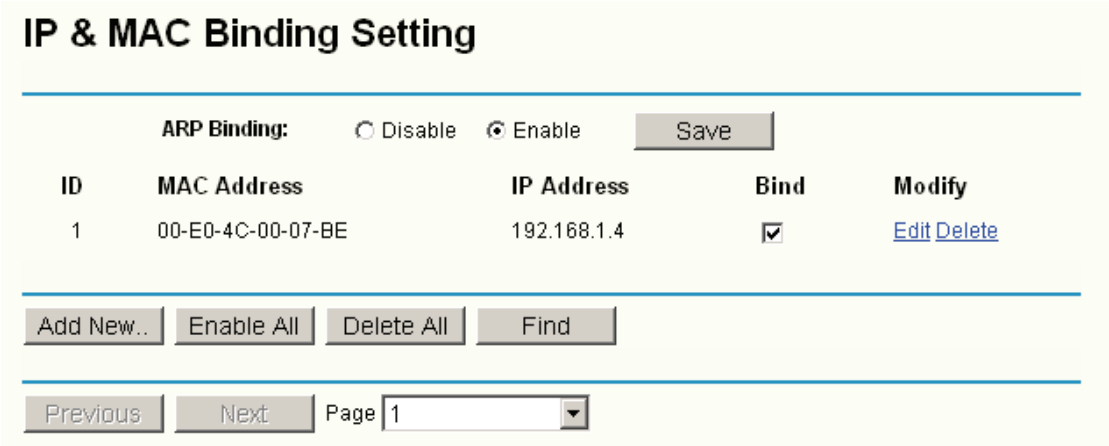


Figure 4-45 IP & MAC Binding Setting

- **MAC Address -** The MAC address of the controlled computer in the LAN.
- **IP Address -** The assigned IP address of the controlled computer in the LAN.
- **Bind -** Whether or not enable the arp binding.
- **Modify -** Edit or delete item.

When you want to add or modify an IP & MAC Binding entry, you can click the **Add New** button or **Modify** button, and then you will go to the next page. This page is used for adding or modifying an IP & MAC Binding entry (shown in Figure 4-46).

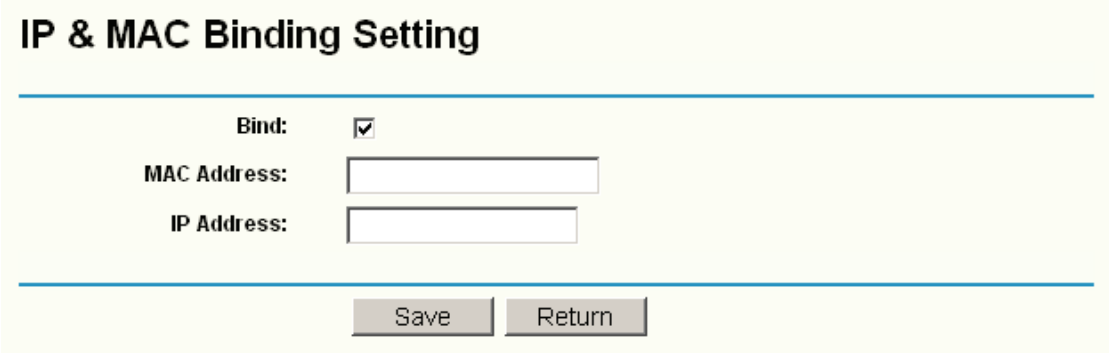


Figure 4-46 IP & MAC Binding Setting (Add & Modify)

To add IP & MAC Binding entries:

1. Click the **Add New...** button.
2. Enter the MAC Address and IP Address.
3. Select the Bind checkbox.
4. Click the **Save** button to save it.

To modify or delete an existing entry:

1. Find the desired entry in the table.
2. Click **Modify** or **Delete** as desired on the **Modify** column.

To find an existing entry:

1. Click the **Find** button (shown in figure 5-43).
2. Enter the MAC Address or IP Address.
3. Enter the **Find** button in the next page (shown in Figure 4-47).

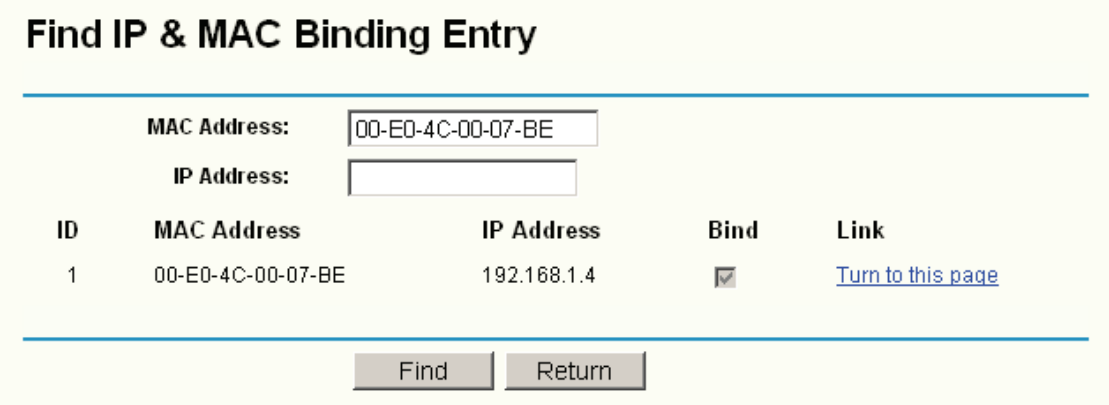


Figure 4-47 Find IP & MAC Binding Entry

Click the **Enable All** button to make all entries enabled.

Click the **Delete All** button to delete all entries.

4.9.2 ARP List

To manage the computer, you could observe the computers in the LAN by checking the relationship of MAC address and IP address on the ARP list, and you could configure the items on the ARP list also. This page displays the ARP List; it shows all the existing IP & MAC Binding entries (shown in Figure 4-48).

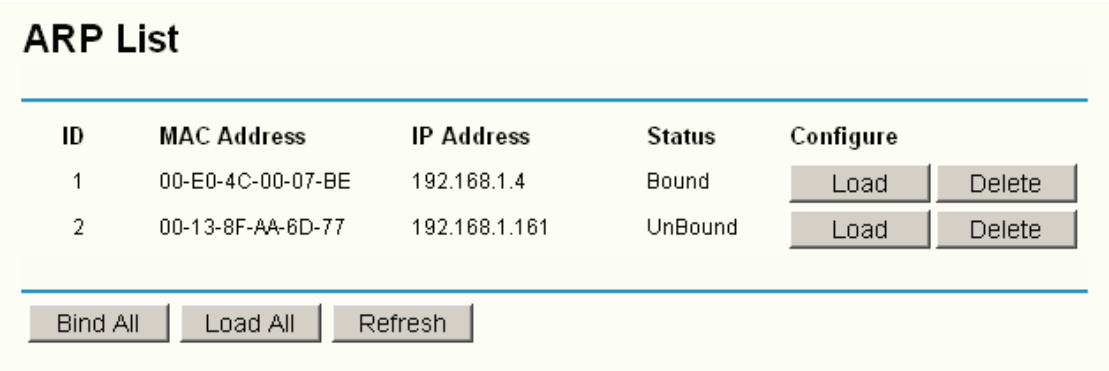


Figure 4-48 ARP List

- **MAC Address** - The MAC address of the controlled computer in the LAN.
- **IP Address** - The assigned IP address of the controlled computer in the LAN.
- **Status** - Enabled or Disabled of the MAC address and IP address binding.
- **Configure** - Load or delete item.
- **Load** - Load the item to the IP & MAC Binding list.
- **Delete** - Delete the item.

Click the **Bind All** button to bind all the current items, available after enable.

Click the **Load All** button to load all items to the IP & MAC Binding list.

Click the **Refresh** button to refresh all items.

☞ **Note:**

An item could not be loaded to the IP & MAC Binding list if the IP address of the item has been loaded before. Error warning will prompt as well. Likewise, "Load All" only loads the items without interference to the IP & MAC Binding list.

4.10 Static Routing

A static route is a pre-determined path that network information must travel to reach a specific host or network. To add or delete a route, work in the area under the Static Routing page (shown in Figure 4-49).

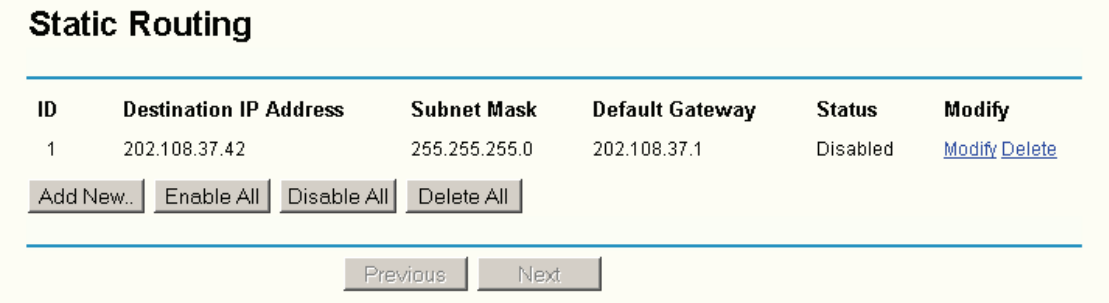


Figure 4-49 Static Routing

To add static routing entries:

1. Click the **Add New** button. (pop-up Figure 4-50)
2. Enter the following data:

- **Destination IP Address -** The **Destination IP Address** is the address of the network or host that you want to assign to a static route.
- **Subnet Mask -** The **Subnet Mask** determines which portion of an IP Address is the network portion, and which portion is the host portion.
- **Gateway -** This is the IP Address of the gateway device that allows for contact between the router and the network or host.

3. Select **Enabled** or **Disabled** for this entry on the **Status** pull-down list.
4. Click the **Save** button to save it.

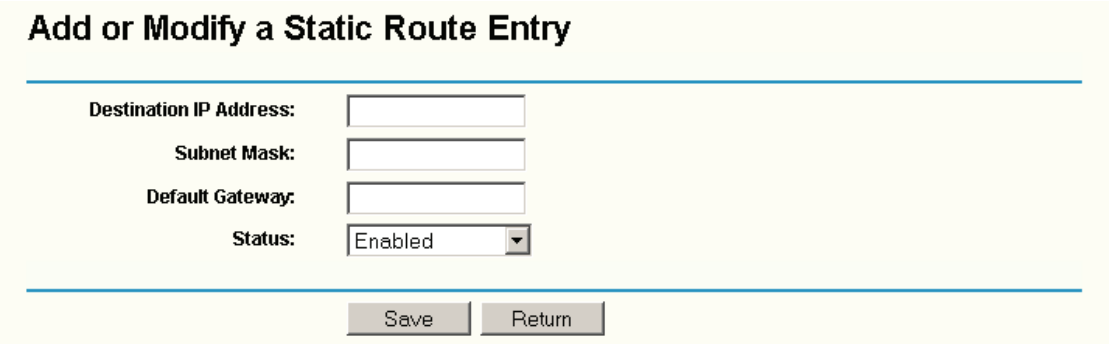


Figure 4-50 Add or Modify a Static Route Entry

To modify or delete an existing entry:

1. Click the **Modify** in the entry you want to modify. If you want to delete the entry, click the **Delete**.
2. Modify the information.
3. Click the **Save** button.

Click the **Enable All** button to make all entries enabled.

Click the **Disabled All** button to make all entries disabled.

Click the **Delete All** button to delete all entries

4.11 DDNS

The router offers a Dynamic Domain Name System (**DDNS**) feature. DDNS lets you assign a fixed host and domain name to a dynamic Internet IP Address. It is useful when you are hosting your own website, FTP server, or other server behind the router. Before using this feature, you need to sign up for DDNS service providers such as www.dyndns.org, www.oray.net or www.comexe.cn. The Dynamic DNS client service provider will give you a password or key.

To set up for DDNS, follow these instructions:

4.11.1 Dyndns.org DDNS

If your selected dynamic DNS **Service Provider** is www.dyndns.org, the page will appear as shown in Figure 4-51:

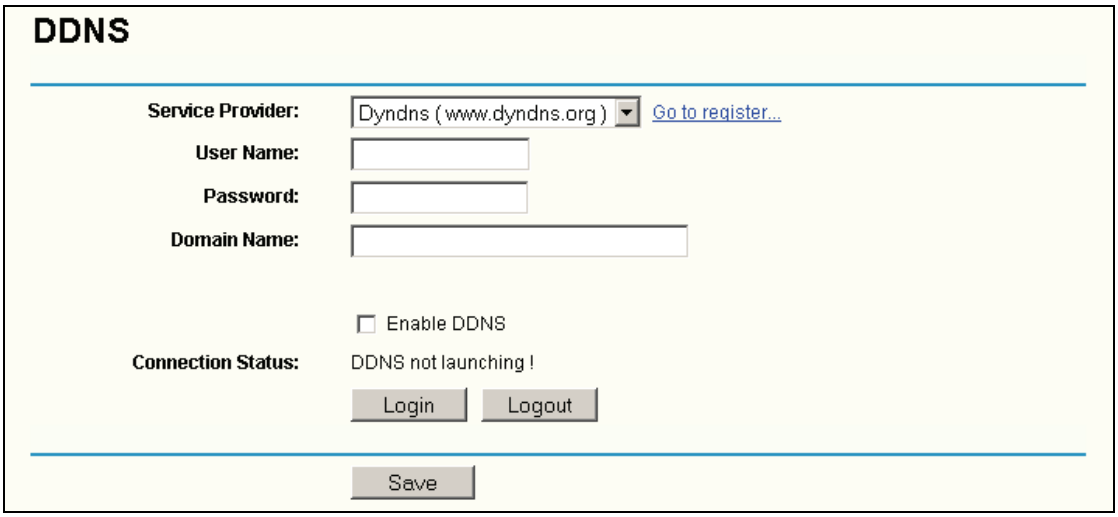


Figure 4-51 Dyndns.org DDNS Settings

To set up for DDNS, follow these instructions:

1. Type the **domain names** your dynamic DNS service provider gave.
2. Type the **User Name** for your DDNS account.
3. Type the **Password** for your DDNS account.
4. Click the **Login** button to login to the DDNS service.

➢ **Connection Status -**The status of the DDNS service connection is displayed here.

Click **Logout** to logout of the DDNS service.

4.11.2 Oray.net DDNS

If your selected dynamic DNS **Service Provider** is www.oray.net, the page will appear as shown in Figure 4-52:

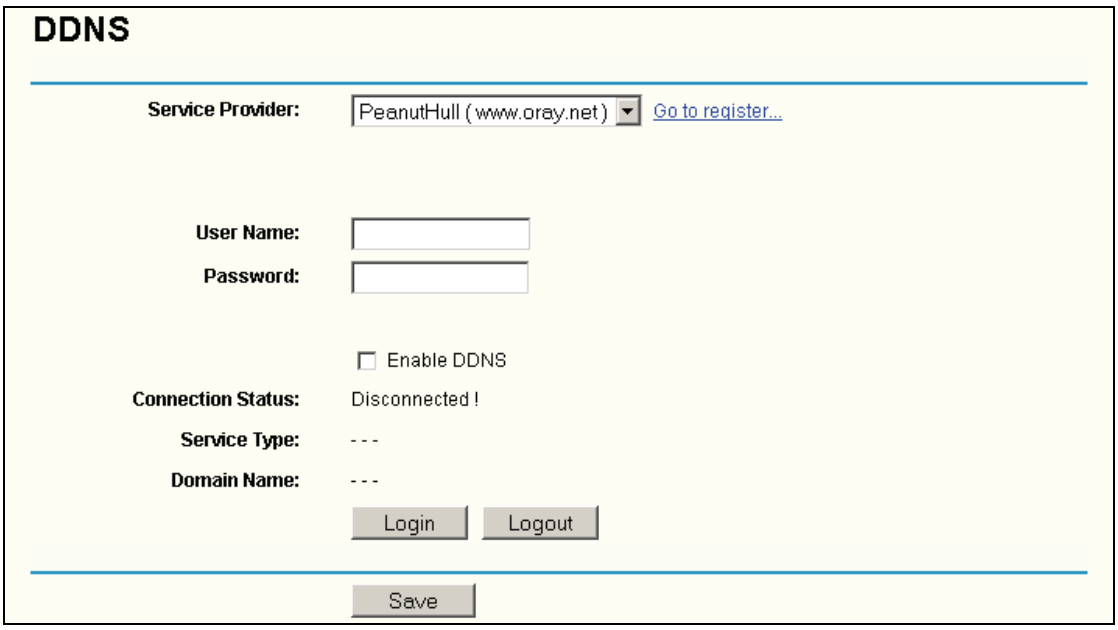


Figure 4-52 Oray.net DDNS Settings

To set up for DDNS, follow these instructions:

1. Type the **User Name** for your DDNS account.
2. Type the **Password** for your DDNS account.
3. Click the **Login** button to login the DDNS service.

   - **Connection Status -** The status of the DDNS service connection is displayed here.
   - **Domain Name -** The domain names are displayed here.

Click **Logout** to logout the DDNS service.

4.11.3 Comexe.cn DDNS

If your selected dynamic DNS **Service Provider** is www.comexe.cn, the page will appear as shown in Figure 4-53:

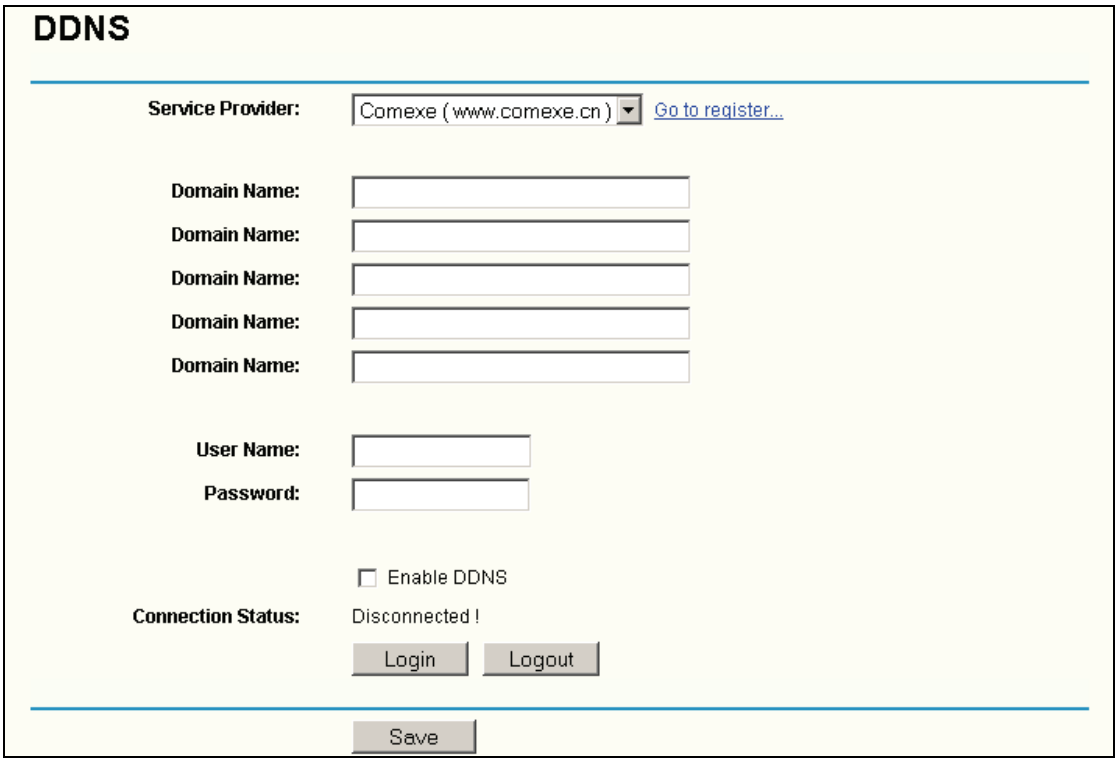


Figure 4-53 Comexe.cn DDNS Settings

To set up for DDNS, follow these instructions:

1. Type the **domain names** your dynamic DNS service provider gave.
2. Type the **User Name** for your DDNS account.
3. Type the **Password** for your DDNS account.
4. Click the **Login** button to login to the DDNS service.

➢ **Connection Status -**The status of the DDNS service connection is displayed here.

Click **Logout** to logout of the DDNS service.

4.12 System Tools

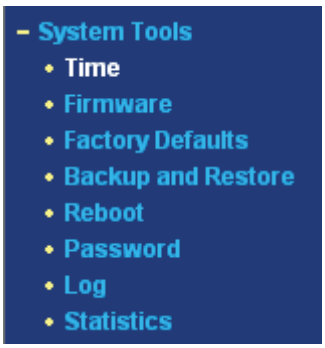


Figure 4-54 The System Tools menu

There are eight submenus under the System Tools menu (shown in Figure 4-54): **Time**, **Firmware**,

Factory Defaults, Backup and Restore, Reboot, Password, Log and **Statistics.** Click any of them, and you will be able to configure the corresponding function. The detailed explanations for each submenu are provided below.

4.12.1 Time

You can set time manually or get GMT from the Internet for the router on this page (shown in Figure 4-55):

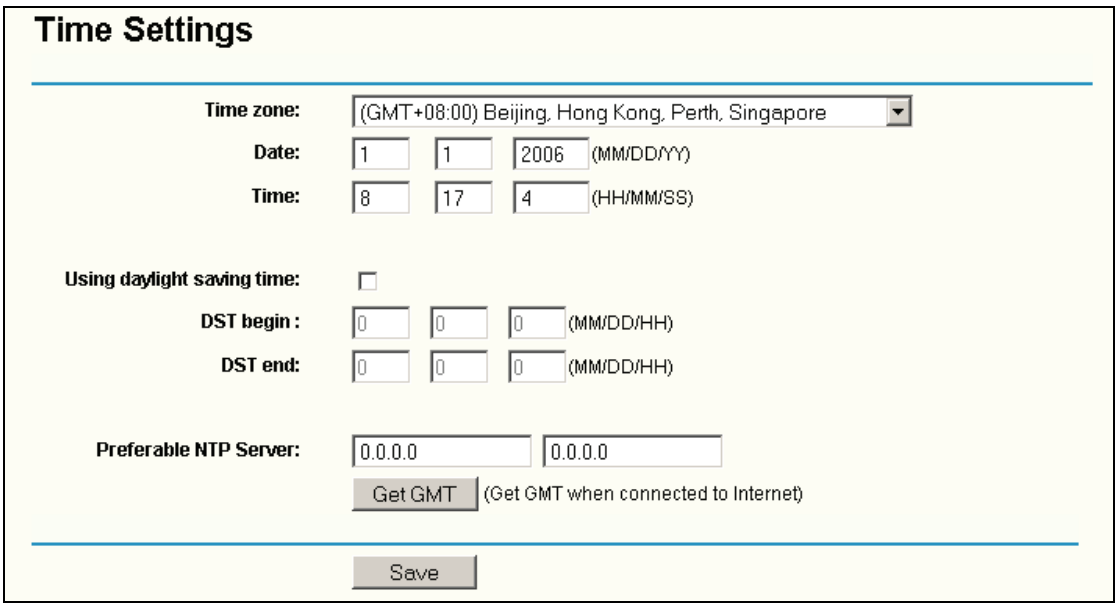


Figure 4-55 Time settings

- **Time Zone -** Select your local time zone from this pull down list.
- **Date -** Enter your local date in MM/DD/YY into the right blanks.
- **Time -** Enter your local time in HH/MM/SS into the right blanks.

Time setting follows these steps below:

1. Select your local time zone.
2. Enter date and time in the right blanks
3. Click **Save**.

Click the **Get GMT** button to get GMT time from Internet if you have connected to Internet.

If you're using Daylight saving time, please follow the steps below.

1. Select **using daylight saving time**.
2. Enter daylight saving beginning time and end time in the right blanks.
3. Click **Save**.

☞ **Note:**

1. This setting will be used for some time-based functions such as firewall. You must specify your time zone once you login to the router successfully, if not, the time limited on these functions will not take effect.
2. The time will be lost if the router is turned off.
3. The router will obtain GMT automatically from Internet if it has already connected to Internet.

4.12.2 Firmware

The page (shown in Figure 4-56) allows you to upgrade the latest version firmware to keep your router up-to-date.

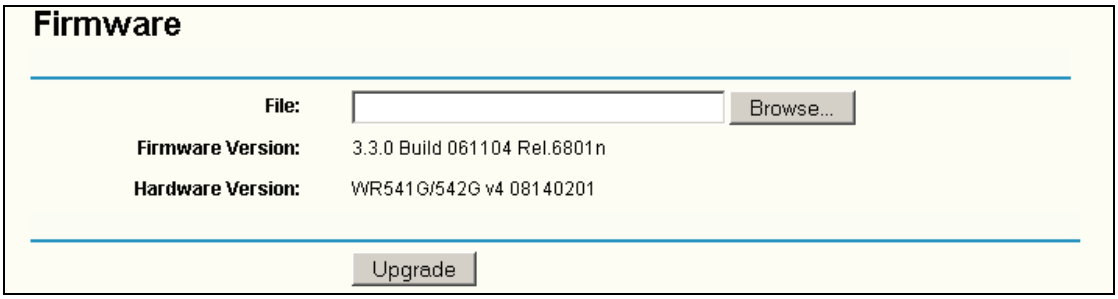


Figure 4-56 Firmware Upgrade

New firmware is posted at www.tp-link.com and can be downloaded for free. If the router is not experiencing difficulties, there is no need to upgrade firmware, unless the new firmware supports a new feature you need.

☞ **Note:**

When you upgrade the router's firmware, you will lose current configuration settings, so make sure you backup the router's settings before you upgrade its firmware.

To upgrade the router's firmware, follow these instructions:

1. Download the latest firmware upgrade file from the TP-LINK website (www.tp-link.com).
2. Click **Browse** to view the folders and select the downloaded file.
3. Click the **Upgrade** button.

- **Firmware Version -** Displays the current firmware version.
- **Hardware Version -** Displays the current hardware version. The hardware version of the upgrade file must accord with the current hardware version.

☞ **Note:**

1. **Do not turn off the router or press the Reset button while the firmware is being upgraded.**

2. The router will reboot after the Upgrading has been finished.

4.12.3 Factory Defaults

This page (shown in Figure 4-57) allows you to restore the factory default settings for the router.

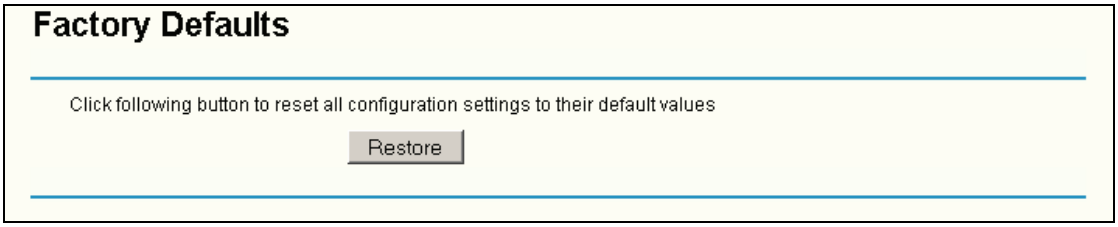


Figure 4-57 Restore Factory Default

Click the **Restore** button to reset all configuration settings to their default values.

- The default **User Name**: admin
- The default **Password**: admin
- The default **IP Address**: 192.168.1.1
- The default **Subnet Mask**: 255.255.255.0

☞ **Note:** Any settings you have saved will be lost when the default settings are restored.

4.12.4 Backup and Restore

This page (shown in Figure 4-58) allows you to save current configuration of router as backup or restore the configuration file you saved before.

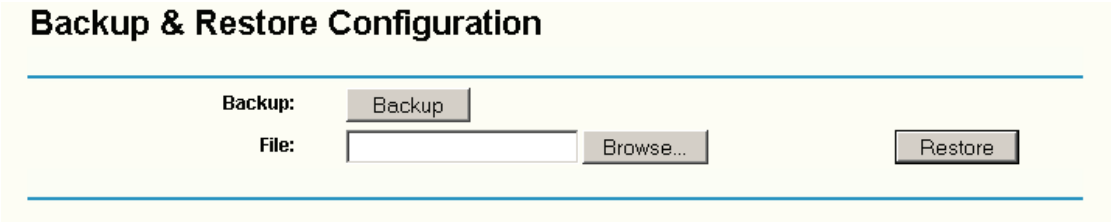


Figure 4-58 Backup & Restore Configuration

- Click the **Backup** button to save all configuration settings as a backup file in your local computer.
- To restore the router's configuration, follow these instructions:

  - Click the **Browse** button to select the backup file which you want to restore.
  - Click the **Restore** button.

☞ **Note:**

The current configuration will be covered with the uploading configuration file. The restoration

process lasts for 20 seconds and the router will restart automatically. Keep the router on during the restoring process, to prevent any damage.

4.12.5 Reboot

This page (shown in Figure 4-59) allows you to reboot the router.

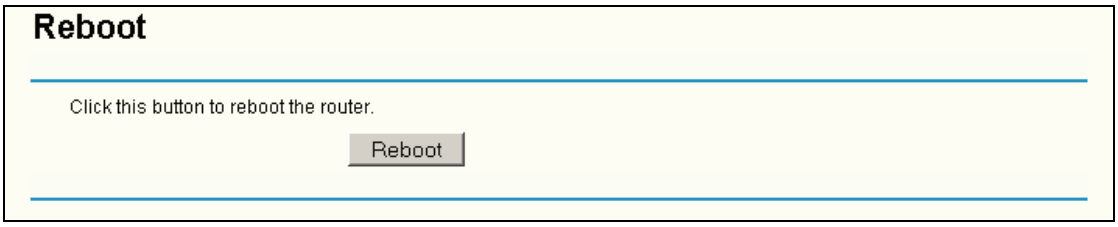


Figure 4-59 Reboot the router

Click the **Reboot** button to reboot the router.

Some settings of the router will take effect only after rebooting, which include:

- Change LAN IP Address. (System will reboot automatically)
- MAC Clone (system will reboot automatically)
- DHCP service function.
- Static address assignment of DHCP server.
- Web Service Port of the router.
- Upgrade the firmware of the router (system will reboot automatically).
- Restore the router's settings to factory default (system will reboot automatically).

4.12.6 Password

This page (shown in Figure 4-60) allows you to change the factory default user name and password of the router.

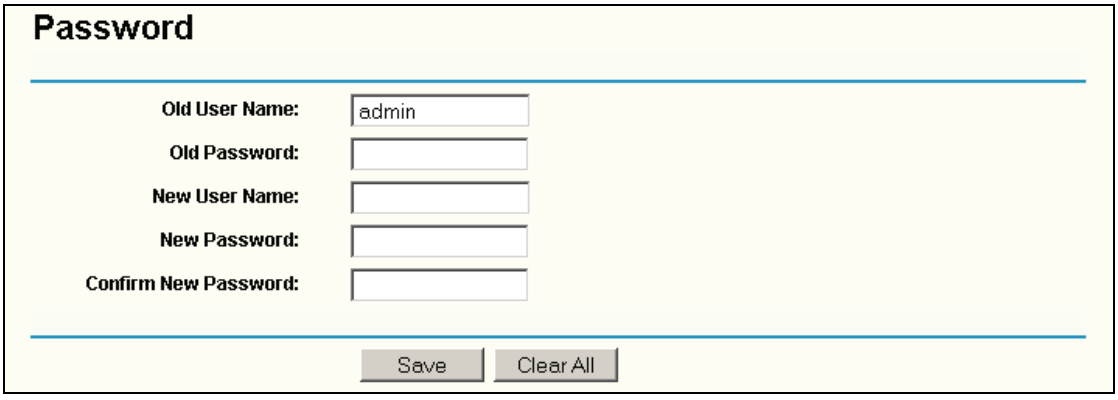


Figure 4-60 Password

It is recommended strongly that you change the factory default user name and password of the

router. All users who try to access the router's Web-based utility or Quick Setup will be prompted for the router's user name and password.

☞ **Note:**

The new user name and password must not exceed 14 characters in length and must not include any spaces. Enter the new Password twice to confirm it.

Click the **Save** button when finished.

Click the **Clear All** button to clear all.

4.12.7 Log

This page (shown in Figure 4-61) allows you to query the logs of the router.

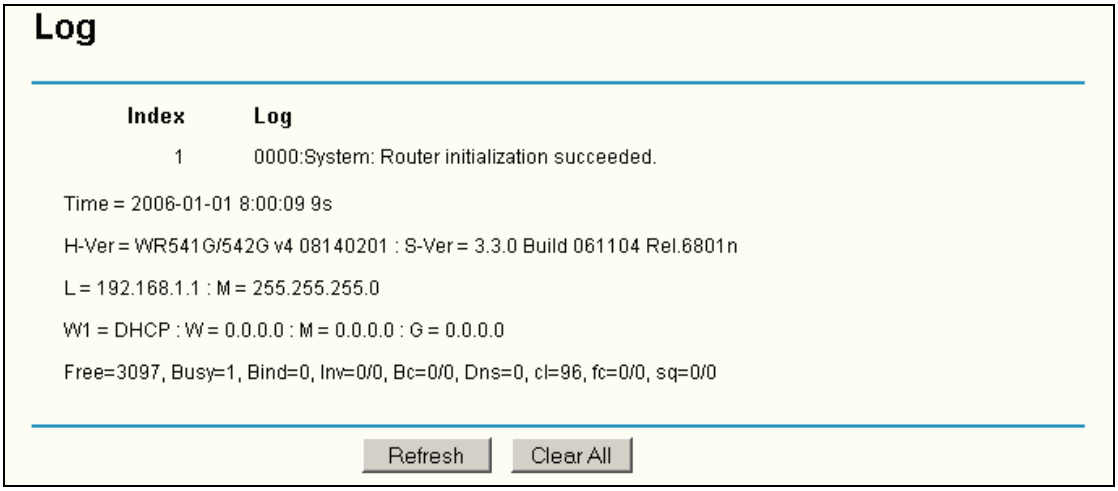


Figure 4-61 System Log

The router can keep logs of all traffic. You can query the logs to find what happened to the router.

Click the **Refresh** button to refresh the logs.

Click the **Clear Log** button to clear all the logs.

4.12.8 Statistics

The Statistics page (shown in Figure 4-62) displays the network traffic of each PC in LAN, including total traffic and traffic of the last **Packets Statistic interval** seconds.

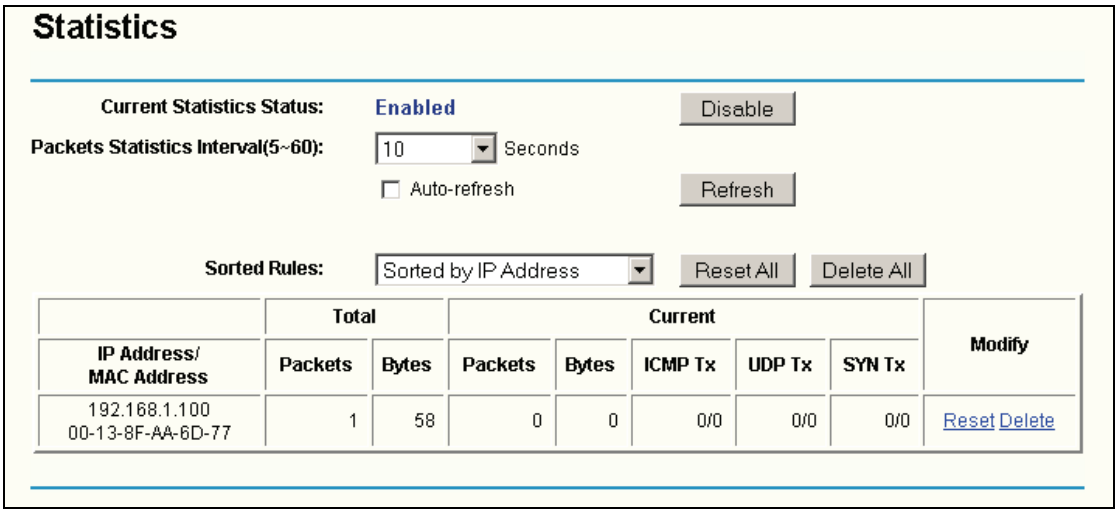


Figure 4-62 Statistics

- **Current Statistics Status -** Enable or Disable. The default value is disabled. To enable, click the **Enable** button. If disabled, the function of DoS protection in Security settings will be ineffective.
- **Packets Statistics Interval -** The default value is 10. Select a value between 5 and 60 seconds in the pull-down list. The Packets Statistic interval indicates the time section of the packets statistic.
- **Sorted Rules -** Here displays sort as desired.

Statistics Table:

IP Address		The IP Address displayed with statistics
Total	**Packets**	The total amount of packets received and transmitted by the router.
	Bytes	The total amount of bytes received and transmitted by the router.
Current	**Packets**	The total amount of packets received and transmitted in the last **Packets Statistic interval** seconds.
	Bytes	The total amount of bytes received and transmitted in the last **Packets Statistic interval** seconds.
	ICMP Tx	The total amount of the ICMP packets transmitted to WAN in the last **Packets Statistic interval** seconds.
	UDP Tx	The total amount of the UDP packets transmitted to WAN in the last **Packets Statistic interval** seconds.
	TCP SYN Tx	The total amount of the TCP SYN packets transmitted to WAN in the last **Packets Statistic interval** seconds.

Click the **Save** button to save the **Packets Statistic interval** value.

Click the **Auto-refresh** checkbox to refresh automatically.

Click the **Refresh** button to refresh immediately.

Appendix A: FAQ

1. How do I configure the router to access Internet by ADSL users?

1) First, configure the ADSL Modem configured in RFC1483 bridge model.

2) Connect the Ethernet cable from your ADSL Modem to the WAN port on the router. The telephone cord plugs into the Line port of the ADSL Modem.

3) Login to the router, click the “Network” menu on the left of your browser, and click "WAN" submenu. On the WAN page, select “PPPoE” for WAN Connection Type. Type user name in the “User Name” field and password in the “Password” field, finish by clicking “Connect”.

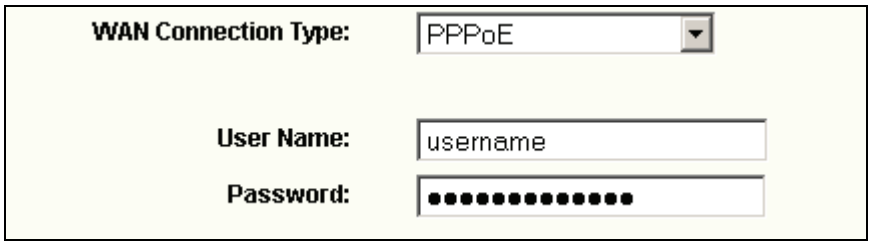


Figure A-1 PPPoE Connection Type

4) If your ADSL lease is in “pay-according-time” mode, select “Connect on Demand” or “Connect Manually” for Internet connection mode. Type an appropriate number for “Max Idle Time” to avoid wasting paid time. Otherwise, you can select “Auto-connecting” for Internet connection mode.

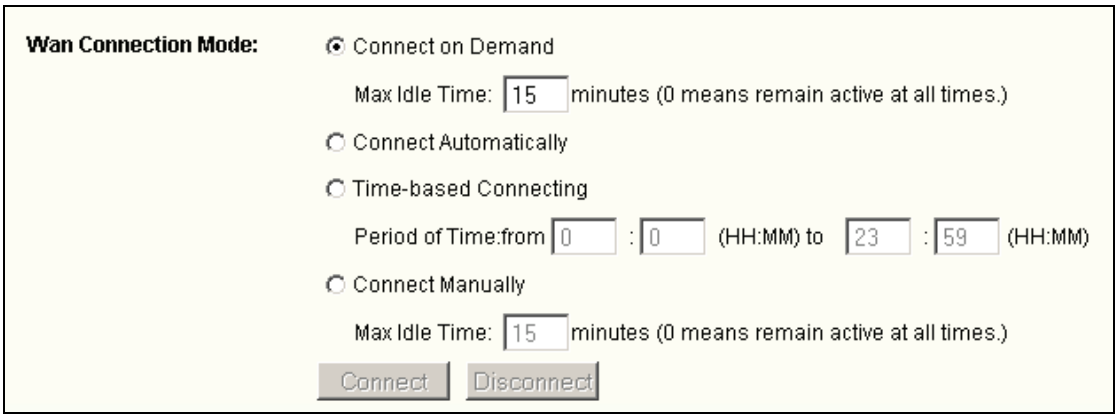


Figure A-2 PPPoE Connection Mode

☞ **Note:**

i. Sometimes the connection cannot be disconnected although you specify a time to Max Idle Time, since some applications is visiting the Internet continually in the background.

ii. If you are a Cable user, please configure the router following the above steps.

2. How do I configure the router to access Internet by Ethernet users?

1) Login to the router, click the “Network” menu on the left of your browser, and click "WAN" submenu. On the WAN page, select “Dynamic IP” for "WAN Connection Type", finish by clicking “Save”.

2) Some ISPs require that you register the MAC Address of your adapter, which is connected to your cable/DSL Modem during installation. If your ISP requires MAC register, login to the router and click the "Network" menu link on the left of your browser, and then click "MAC Clone" submenu link. On the "MAC Clone" page, if your PC’s MAC address is proper MAC address, click the "Clone MAC Address" button and your PC’s MAC address will fill in the "WAN MAC Address" field. Or else, type the MAC Address into the "WAN MAC Address" field. The format for the MAC Address is XX-XX-XX-XX-XX-XX. Then click the "Save" button. It will take effect after rebooting.

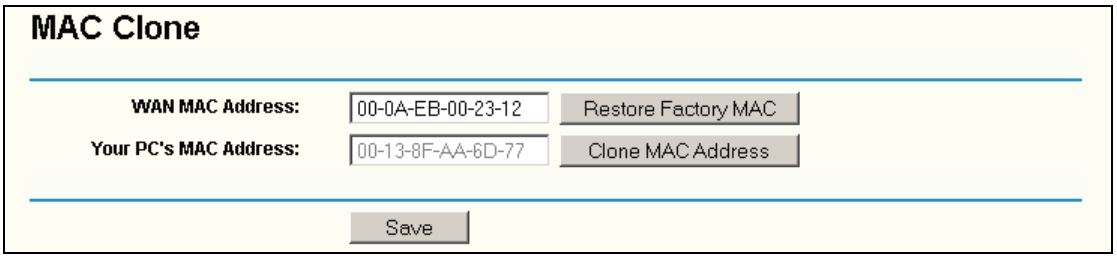


Figure A-3 MAC Clone

3. I want to use Netmeeting, what do I need to do?

1) If you start a Netmeeting as a host, no configuration is needed but entering the invitee’s IP address.

2) If you start a Netmeeting as an invitee, you need to configure Virtual Server or DMZ Host first.

3) How to configure Virtual Server: Login to the router, click the “Forwarding” menu on the left of your browser, and click "Virtual Servers" submenu. On the "Virtual Server" page, click **Add New,** then on the “Add or Modify a Virtual Server” page, enter “1720” into the blank behind the “Service Port”, and your IP address behind the IP Address, assuming 192.168.1.169 for an example, remember to “Enable” and “Save”.



Figure A-4 Virtual Servers

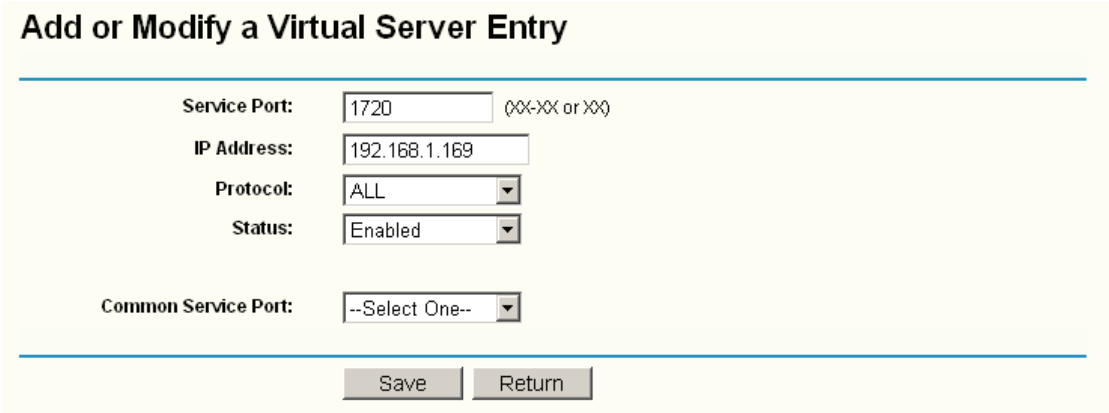


Figure A-5 Add or Modify a Virtual server Entry

Note:

Your opposite side should call your WAN IP, which is displayed on the “Status” page.

4) How to enable DMZ Host: Login to the router, click the “Forwarding” menu on the left of your browser, and click "DMZ" submenu. On the "DMZ" page, click “Enable” radio and type your IP address into the “DMZ Host IP Address” field, using 192.168.1.169 as an example, remember to click the "Save” button.

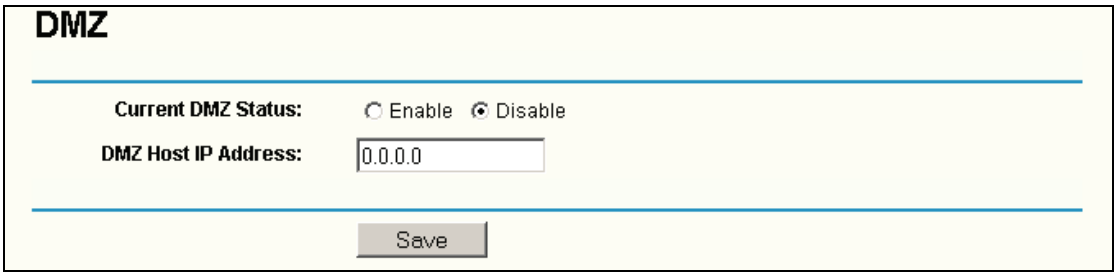


Figure A-6 DMZ

4. I want to build a WEB Server on the LAN, what should I do?

1) Because the WEB Server port 80 will interfere with the WEB management port 80 on the router, you must change the WEB management port number to avoid interference.

2) To change the WEB management port number: Login to the router, click the “Security” menu on the left of your browser, and click "Remote Management" submenu. On the "Remote Management" page, type a port number except 80, such as 88, into the "Web

Management Port" field. Click “Save” and reboot the router.

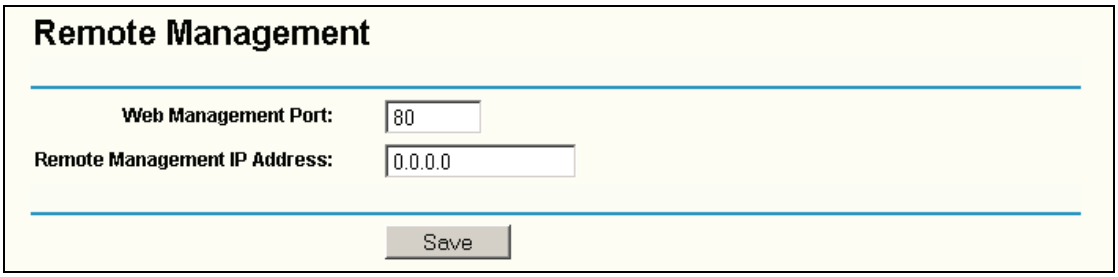


Figure A-7 Remote Management

Note:

If the above configuration takes effect, to configure to the router by typing http://192.168.1.1:88 (the router’s LAN IP address: Web Management Port) in the address field of the Web browser.

3) Login to the router, click the “Forwarding” menu on the left of your browser, and click the "Virtual Servers" submenu. On the "Virtual Server" page, click **Add New,** then on the “Add or Modify a Virtual Server” page, enter “80” into the blank behind the “Service Port”, and your IP address behind the IP Address, assuming 192.168.1.188 for an example, remember to “Enable” and “Save”.

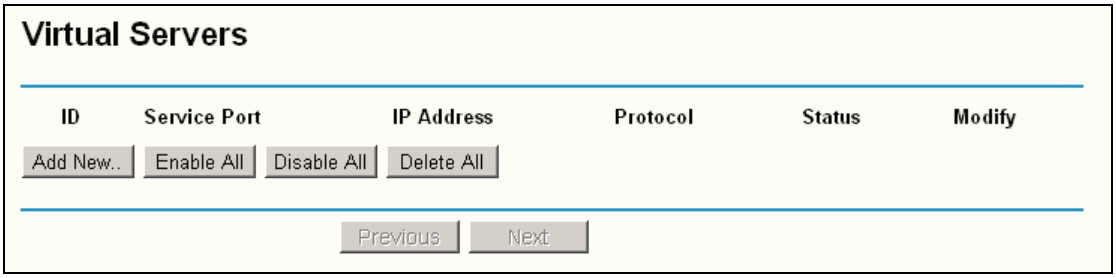


Figure A-8 Virtual Servers

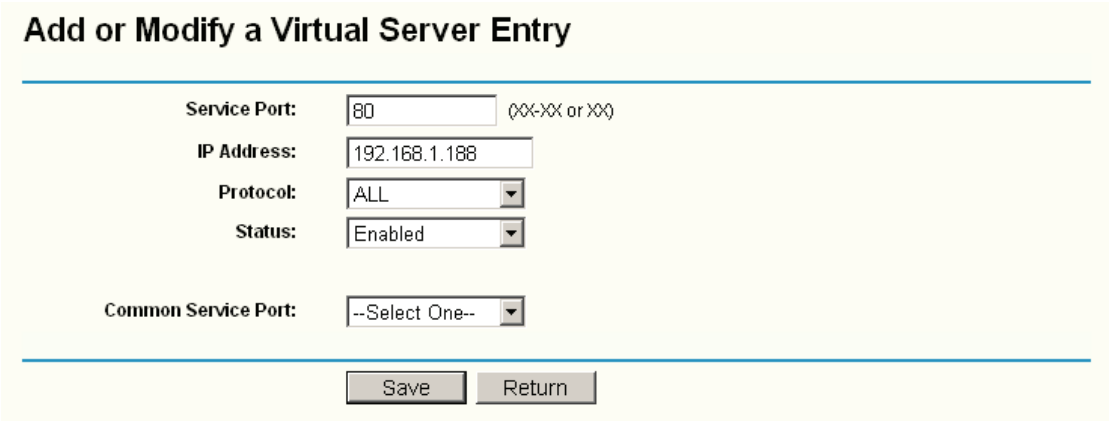


Figure A-9 Add or Modify a Virtual server Entry

5. The wireless stations cannot connect to the router.

1) Make sure the "Wireless Router Radio" is enabled.

2) Make sure that the wireless stations' SSID accord with the router's SSID.

3) Make sure the wireless stations have right KEY for encryption when the router is encrypted.

4) If the wireless connection is ready, but you can't access the router, check the IP Address of your wireless stations.

Appendix B: Configuring the PC

In this section, we'll introduce how to install and configure the TCP/IP correctly in Windows XP. First make sure your Ethernet Adapter is working, refer to the adapter's manual if needed.

1. Install TCP/IP component

1) On the Windows taskbar, click the **Start** button, point to **Settings**, and then click **Control Panel**.

2) Click the **Network and Internet Connections** icon, and then click on the **Network Connections** tab in the appearing window.

3) Right click the icon that showed below, select Properties on the prompt page.

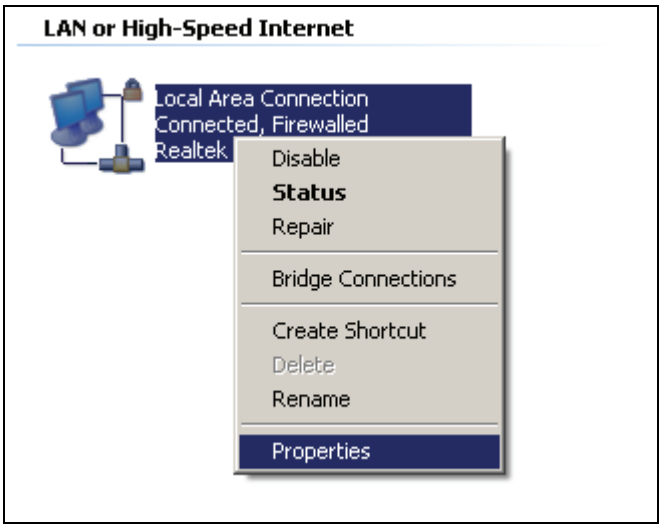


Figure 1

4) In the prompt page that showed below, double click on the **Internet Protocol (TCP/IP)**.

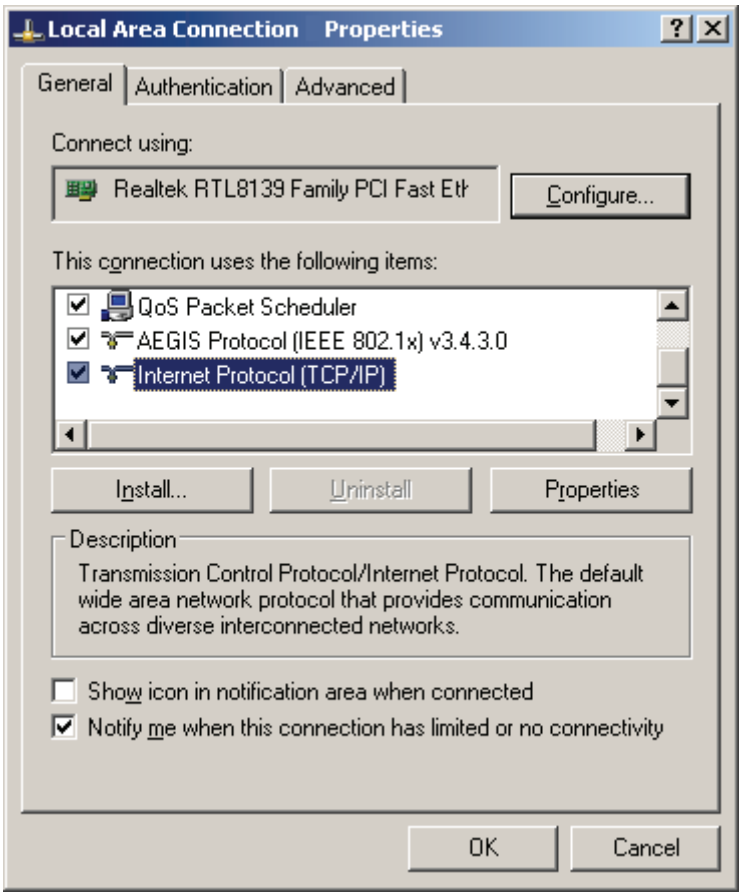


Figure 2

5) The following **TCP/IP Properties** window will display and the **IP Address** tab is open on this window by default.

Now you have two ways to configure the **TCP/IP** protocol below:

➢ **Setting IP address automatically**

Select **Obtain an IP address automatically**, Choose **Obtain DNS server automatically**, as shown in the Figure below:

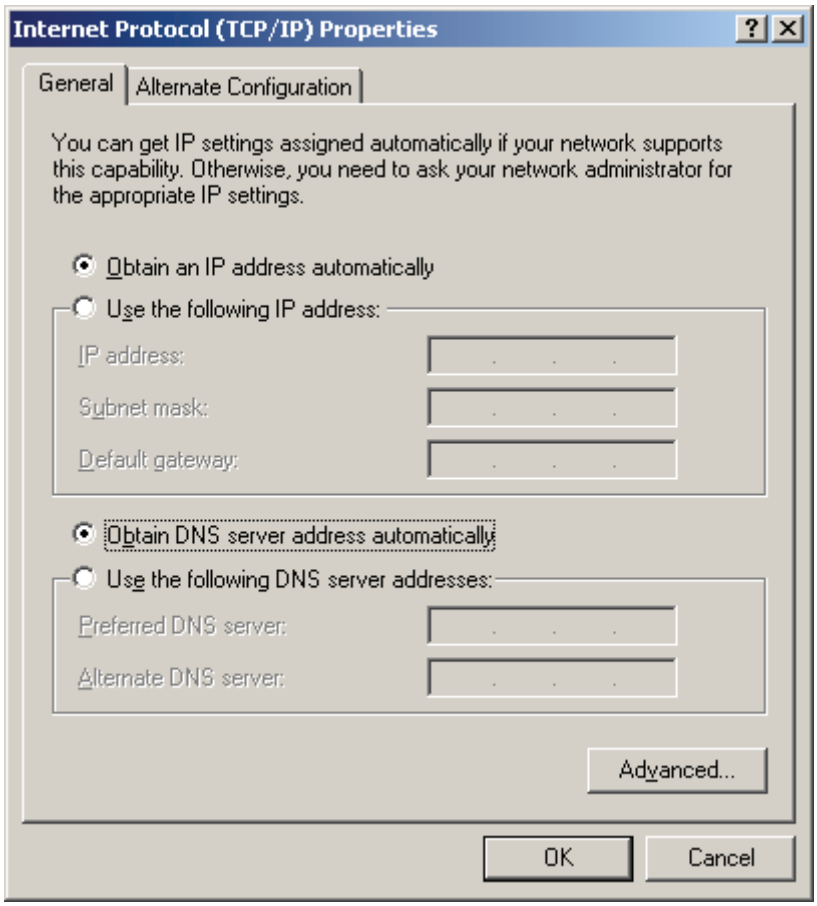


Figure 3

➢ **Setting IP address manually**

1 Select **Use the following IP address** radio button. And the following items available

2 If the router's LAN IP address is 192.168.1.1, type IP address is 192.168.1.x (x is from 2 to 254), and **Subnet mask** is 255.255.255.0.

3 Type the router's LAN IP address (the default IP is 192.168.1.1) into the **Default gateway** field.

4 Select **Use the following DNS server addresses** radio button. In the **Preferred DNS Server** field you can type the DNS server IP address, which has been provided by your ISP

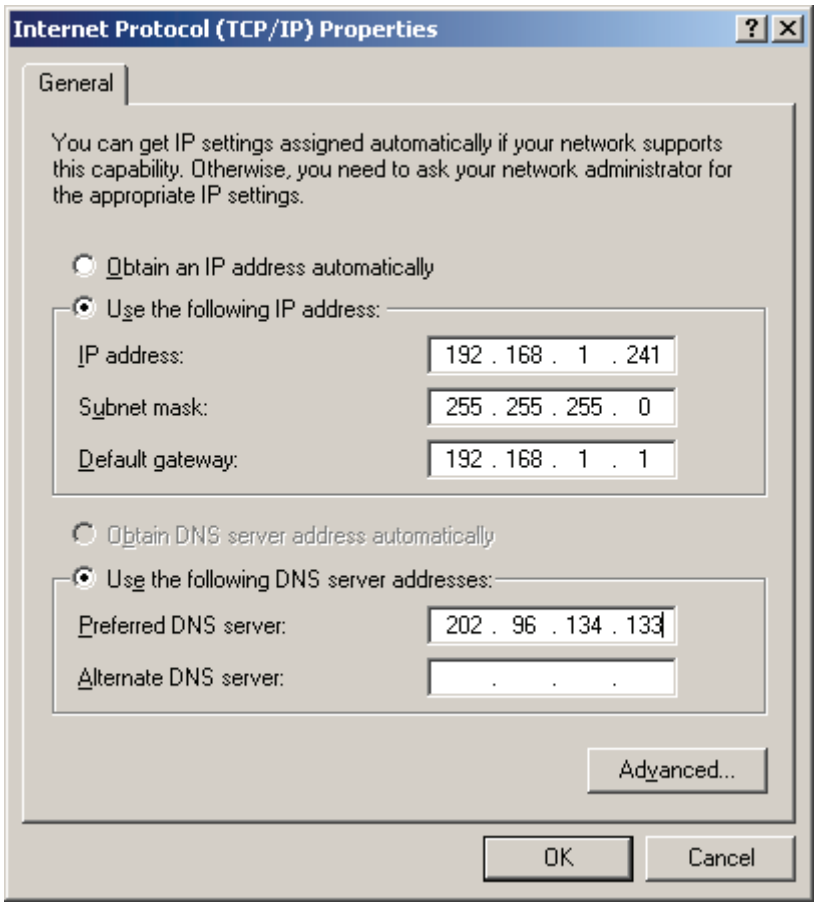

Internet Protocol (TCP/IP) Properties
General
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address: 192 . 168 . 1 . 241
Subnet mask: 255 . 255 . 255 . 0
Default gateway: 192 . 168 . 1 . 1
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server: 202 . 96 . 134 . 133
Alternate DNS server:
Advanced...
OK
Cancel

Figure 4

Appendix C: Specifications

General	
Standards	IEEE 802.3, 802.3u, 802.11b and 802.11g
Protocols	TCP/IP, PPPoE, DHCP, ICMP, NAT, SNTP
Ports	One 10/100M Auto-Negotiation WAN RJ45 port, Four 10/100M Auto-Negotiation LAN RJ45 ports supporting Auto MDI/MDIX
Cabling Type	10BASE-T: UTP category 3, 4, 5 cable (maximum 100m) EIA/TIA-568 100Ω STP (maximum 100m) 100BASE-TX: UTP category 5, 5e cable (maximum 100m) EIA/TIA-568 100Ω STP (maximum 100m)
Radio Data Rate	54/48/36/24/18/12/9/6Mbps or 11/5.5/3/2/1Mbps
LEDs	Power, SYS, WLAN, WAN, 1-4
Safety & Emissions	FCC, CE

Environmental and Physical	
Operating Temp.	0℃~40℃ (32℉~104℉)
Operating Humidity	10% - 90% RH, Non-condensing
Dimensions (W×D×H)	6.9×4.4×1.2 in. (174×111×30 mm) (without antenna)

Appendix D: Glossary

- **2x to 3x eXtended Range™ WLAN Transmission Technology -** The WLAN device with 2x to 3x eXtended Range™ WLAN transmission technology make its sensitivity up to 105 dB, which gives users the ability to have robust, longer-range wireless connections. With this range-enhancing technology, a 2x to 3x eXtended Range™ based client and access point can maintain a connection at as much as three times the transmission distance of traditional 802.11b and 802.11g products, for a coverage area that is up to nine times greater. A traditional 802.11b and 802.11g product transmission distance is about 300m, a 2x to 3x eXtended Range™ based client and access point can maintain a connection transmission distance may be up to 830m.
- **802.11b -** The 802.11b standard specifies a wireless networking at 11 Mbps using direct-sequence spread-spectrum (DSSS) technology and operating in the unlicensed radio spectrum at 2.4GHz, and WEP encryption for security. 802.11b networks are also referred to as Wi-Fi networks.
- **802.11g -** specification for wireless networking at 54 Mbps using direct-sequence spread-spectrum (DSSS) technology, using OFDM modulation and operating in the unlicensed radio spectrum at 2.4GHz, and backward compatibility with IEEE 802.11b devices, and WEP encryption for security.
- **DDNS** (**D**ynamic **D**omain **N**ame **S**ystem) **-** The capability of assigning a fixed host and domain name to a dynamic Internet IP Address.
- **DHCP** (**D**ynamic **H**ost **C**onfiguration **P**rotocol) **-** A protocol that automatically configure the TCP/IP parameters for the all the PC(s) that are connected to a DHCP server.
- **DMZ** (**Dem**ilitarized **Z**one) **-** A Demilitarized Zone allows one local host to be exposed to the Internet for a special-purpose service such as Internet gaming or videoconferencing.
- **DNS** (**D**omain **N**ame **S**ystem) **–** An Internet Service that translates the names of websites into IP addresses.
- **Domain Name -** A descriptive name for an address or group of addresses on the Internet.
- **DoS** (**D**enial **o**f **S**ervice) **-** A hacker attack designed to prevent your computer or network from operating or communicating.
- **DSL** (**D**igital **S**ubscriber **L**ine) **-** A technology that allows data to be sent or received over existing traditional phone lines.
- **ISP** (**I**nternet **S**ervice **P**rovider) **-** A company that provides access to the Internet.
- **MTU** (**Maximum Transmission Unit**) **-** The size in bytes of the largest packet that can be

transmitted.

- **NAT** (**N**etwork **A**ddress **T**ranslation) **-** NAT technology translates IP addresses of a local area network to a different IP address for the Internet.
- **PPPoE** (**P**oint to **P**oint **P**rotocol **o**ver **E**thernet) **-** PPPoE is a protocol for connecting remote hosts to the Internet over an always-on connection by simulating a dial-up connection.
- **SSID -** A **S**ervice **S**et **Id**entification is a thirty-two character (maximum) alphanumeric key identifying a wireless local area network. For the wireless devices in a network to communicate with each other, all devices must be configured with the same SSID. This is typically the configuration parameter for a wireless PC card. It corresponds to the ESSID in the wireless Access Point and to the wireless network name.
- **WEP** (**W**ired **E**quivalent **P**rivacy) **-** A data privacy mechanism based on a 64-bit or 128-bit or 152-bit shared key algorithm, as described in the IEEE 802.11 standard.
- **Wi-Fi -** A trade name for the 802.11b wireless networking standard, given by the Wireless Ethernet Compatibility Alliance (WECA, see http://www.wi-fi.net), an industry standards group promoting interoperability among 802.11b devices.
- **WLAN** (**W**ireless **L**ocal **A**rea **N**etwork) **-** A group of computers and associated devices communicate with each other wirelessly, which network serving users are limited in a local area.

http://www.tp-link.com